U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed $25.00.

If all potentially responsive pages are released on CD, you will owe $40.00 in duplication fees (3 CDs at $15.00 each, less $5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe $79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a $5.00 credit towards your first interim CD. As a result, we must notify you there will be a $25.00 charge when the second interim release is made in this case. At that time you will be billed for the $10.00 remaining from the $15.00 free of the first release, as well as the $15.00 duplication fee for the second release, for a total of $25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

FBI taps of e-mail provoke concerns

Privacy issues lead to House hearings on 'Carnivore' work; Name called 'unfortunate'

By Del Quentin Wilber
Sun National Staff

WASHINGTON -- To civil libertarians and Internet service providers, a device created by the FBI to snoop through e-mail messages is as ominous as its name: "Carnivore."

Attached to an ISP's server, the contraption sifts through countless e-mail messages and copies specific information for federal agents seeking suspected criminals, including terrorists and child pornographers.

But critics say that, in the process of sifting out communications from its targets, Carnivore is also capable of retrieving the private messages of innocent people.

"This is a very dangerous device," said Barry Steinhardt, associate director of the American Civil Liberties Union. "It's unprecedented. It's the first time law enforcement has carte blanche access to the entire service provider's network."

The controversy surrounding the device with the foreboding name has caught the attention of Republican lawmakers, and a House Judiciary subcommittee is scheduled to hold a hearing on the matter today. Opponents and authorities who support the use of Carnivore are scheduled to testify.

After the system was disclosed in recent news accounts, sparking criticism from privacy advocates, FBI officials met with lawmakers and reporters to try to show that Carnivore is not nearly as intrusive as some fear.

For one thing, FBI officials said, they need the device to combat crime and threats to national security. They describe Carnivore as a "surgical" tool that would protect ordinary people from unintended searches.

"There are filtering mechanisms built in that limit the amount of information viewable to the human eye," said Paul Bresson, a spokesman for the bureau. "It ensures that only the exact communications authorized by a court are what we intercept."

For decades, federal agents and local police have been wiretapping suspects' phones after obtaining permission from judges. But those wiretaps are limited to a specific suspect and do not comb through phone calls at random.

Carnivore works much differently, though authorities still must obtain permission from a judge to scour e-mail messages or discover which Web pages a suspect visits.

Once they have court approval, agents attach the Carnivore device -- an

DOC. #20

ordinary-looking desktop computer -- to the ISP's main computer, and Carnivore "passively" sniffs through streams of data, FBI officials said.

Carnivore does not read e-mail messages or their subject lines, officials said. Instead, it searches for computer codes that direct the message to and from the suspect. Nor can it scan e-mail messages for key words, like "drugs or bomb," an FBI official said.

In other words, authorities say, Carnivore acts like an FBI agent authorized to scan envelopes sent by mail. The agent seeks a particular suspect's addressing information and pulls aside any qualified envelope and opens it.

Last week, after an outcry from critics, the White House said it would propose legislation to, among other things, require agents to seek Justice Department clearance before asking judges to authorize the use of Carnivore in a specific case. Such rules already cover voice wiretaps.

But the proposal was dismissed by civil liberties groups, who said it did not go far enough in protecting electronic communication.

For their part, FBI officials say, the White House proposal is not necessary: They say they abide by the rules governing voice wiretaps to use Carnivore.

Despite the assurances of FBI officials, civil liberties groups and congressional Republicans say they are wary of the system.

"It has the capability of grabbing it all," said Richard Diamond, a spokesman for Rep. Dick Armey, the Texas Republican who is the House majority leader and a sharp critic of Carnivore. "It all depends on who pushes the button. Someone could push the wrong button and have access to all sorts of information."

FBI officials dispute that assertion, though they concede that Carnivore has sometimes captured e-mail messages and data that were not targeted in their searches. They say they sealed such information and did not read it.

Earlier this year, an ISP tried unsuccessfully to prevent FBI agents from installing Carnivore on its network. After a brief court fight, the company, Earthlink, yielded to FBI demands and helped install the device.

FBI officials say they don't mind simply asking ISPs to provide them with e-mail sent by criminal suspects if that is possible. But, in most cases, agents would rather use Carnivore because it helps maintain security for criminal evidence. And many smaller ISPs are not capable of creating programs to obtain the necessary data, FBI officials said.

Though most ISPs have complied with court orders to install Carnivore, one major provider said it would refuse.

"We're not going to stand for this," said William L. Schrader, chairman and chief executive officer of PSINet Inc. "It's insidious. If they were to ask us with a court order to violate the privacy of all our customers, we would take this to the Supreme Court."

Authorities say that more criminals, especially those involved in child pornography and fraud, are increasingly using the Internet and e-mail to commit crimes.

About three years ago, agents and federal prosecutors began asking for real-time access to e-mail and Web-site visits, FBI officials said. The agents said they were worried about not having reliable and up-to-date intelligence.

FBI technicians began developing Carnivore, which was used for the first time about 18 months ago, authorities said. FBI officials declined to disclose any information about Carnivore-related cases but said the system has been used fewer than 25 times.

FBI officials said the "unfortunate" choice of a name emerged during internal discussions of the program. At first, technicians called it "Omnivore" because it ate everything in sight. But as the system became more refined, technicians felt it needed a better name and changed it to Carnivore: a meat-eater.

"We're looking at how we name a lot of projects right now," an FBI official said. "This has been sobering."

FBI agents noted that they don't need Carnivore to read most old e-mail messages stored on ISP servers; they can already do so with court approval.

They described the Carnivore system as a last-resort measure to capture real-time communications.

Authorities on technology and society say they are hardly surprised that the system has generated anxiety, because many people now send more personal information over e-mail than over the phone.

Corporate snooping of employee e-mail and the unauthorized sale of client information by e-retailers have unnerved many computer users.

Originally published Jul 24 2000

USA TODAY Tech Report

provided by Bloomberg

07/21/00- Updated 04:19 PM ET

Send this story to a friend

FBI: 'Carnivore' will play nice

During demonstration, details of e-mail 'wiretap' system emerge

WASHINGTON (Bloomberg) — The FBI's Carnivore e-mail surveillance system won't snoop on innocent Internet users, officials said Friday.

FBI officials gave reporters a demonstration of the system they say adopts traditional telephone wiretap methods to the Internet without violating the rights of law-abiding Web surfers.

From our archive:

- Clinton proposes updated wiretap laws
- FBI e-mail snooping sparks controversy
- Reno reviewing FBI's Net 'wiretap' system

The disclosure that the FBI and Internet service providers have cooperated to bug the messages of criminal suspects has generated criticism from civil liberties groups and some Republican lawmakers. They say Carnivore will let the FBI see e-mails of all Internet subscribers, not just the few suspects the FBI wants to track.

FBI officials will defend Carnivore Monday before a U.S. House Judiciary subcommittee headed by Republican Henry Hyde of Illinois.

Earlier this week, the Clinton administration proposed limiting law enforcement wiretapping of e-mail to investigations of serious crimes and requiring top-level Justice Department authorization of e-mail

Search
the site the Web
GO
POWERED BY LYCOS

Inside Tech
Talk Tech
FAQ/Tips
Web Column
Hot Sites
Tech News
Tech Investor
Tech Reviews
Answer Desk
Game Zone

Daily Digest
Shareware Shelf
Web Potholes
Web Resources
Consumer Sites
Tech Front

Marketplace
Hardware
Accessories
Software

Print Edition
Today
Yesterday
Subscribe
Archive

Resources
E-mail
Site map
Feedback
About us
Jobs at USA TODAY

Free premiums
USA TODAY Update Software

USA TODAY .com Users!

bugging. Under proposed legislation, the procedures for e-mail surveillance would be similar to those in place for telephone surveillance.

Court order

Electronic tapping of an Internet service provider's data traffic requires a court order. No judge has rejected the government's application for a court order to connect Carnivore to the computer servers of private Internet companies.

These servers contain mountains of data traffic generated by millions of subscribers. Internet companies generally let FBI officials who come to their offices monitor the companies' Internet messages, FBI officials said.

The FBI said it's looking for two academic institutions to serve as outside auditors to ensure the FBI doesn't overreach its authority and pry into the online communications of the general public.

FBI officials said Carnivore has been used 25 times in the past year. It was introduced three years ago.

Carnivore uses a "filter," which is a computer containing proprietary software the FBI buys from private companies. The filter will connect to the servers of Internet companies to weed out messages sent and received by people unconnected to the investigation, officials said, speaking on condition of anonymity. They said the Carnivore filter blocks law-enforcement officials from seeing the e-mail of innocent bystanders.

Big Internet companies already have their own filtering systems that screen messages to be seen by the FBI and spare agents from reviewing extraneous data, officials said.

Front page, News, Sports, Money, Life, Weather, Marketplace

GOP.gov

HOUSE REPUBLICAN CONFERENCE

J.C. WATTS, JR.
CHAIRMAN
4th District, Oklahoma

Reforming Washington
Securing America's Future

News Release

For Immediate Release
Monday, July 24, 2000

Contact: Ron Bonjean/Kevin Schweers
(202) 225-5107

Watts: FBI's 'Carnivore' System a Dangerous Invasion of Privacy

Calls on Clinton-Gore Administration to Suspend New Surveillance Program

WASHINGTON – Rep. J.C. Watts, Jr. (R-OK), Chairman of the House Republican Conference and House Republican Cyber-Security Team, issued the following statement today on the FBI's "Carnivore" system at a Capitol Hill hearing:

"We need innovative, new law enforcement strategies to combat the real and growing threat of cyber-crime. U.S. law enforcement needs to focus resources on the training and expertise necessary to protect our cyber-security. I remain committed to working in Congress to adequately invest in and support the right law enforcement tactics.

"However, the FBI's 'Carnivore' program represents a dangerous and unprecedented invasion of online privacy. Despite repeated inquiries, the Clinton-Gore Administration continues to offer only vague responses and little enlightenment.

"The FBI's record on protecting privacy is also problematic. From unwarranted wiretaps to its mishandling of hundreds of files on political appointees just a few years ago, there is ample cause for concern.

"Before we impose privacy restrictions on the commercial industry, it seems the federal government has a duty and an obligation to honor the privacy of the people it has sworn to protect. I commend Chairman Canady for highlighting this egregious threat to the online privacy of every American."

-- END --

House Committee

FBI E-Mail Surveillance Program

Judiciary
Washington, District of Columbia (United States)
Rayburn House Office Building,
ID: 158376 - 07/24/2000 - 2:00 - No Sale

Hyde, Henry J., U.S. Representative, R-IL
Baker, Stewart, Attorney
Corn-Revere, Robert, Attorney
DiGregory, Kevin, Deputy Assistant Attorney Gene, Department of Justice
Steinhardt, Barry, Associate Director, American Civil Liberties Union
Kerr, Donald, Director, Federal Bureau of Investigation, Crime Lab

Committee members hear testimony on a computer program called 'Carnivore' that will allow the FBI to intercept and collect electronic communications that are the subject of court orders.

For more information please contact viewer@c-span.org.

Doc. #23

C-SPAN Networks
Schedule for Monday, 07/24/2000

All Times E.D.T.

Fri Sat Sun Mon Tue Wed Thu

Previous Day 07 / 24 / 2000 Go! Next Day

Current 3 Months
Search the C-SPAN Schedule

Back to Current Schedule

C-SPAN

Time	Program
07:00 am (est.)	Call-In 1:15 Open Phones C-SPAN, Washington Journal *LIVE*
08:15 am (est.)	Call-In 0:45 Diplomatic Meetings C-SPAN, Washington Journal Massimo Calabresi , *TIME* Magazine *LIVE*
09:00 am (est.)	Call-In 0:30 The History of Philadelphia C-SPAN, Washington Journal *LIVE*
09:30 am (est.)	Call-In 0:30 Benjamin Franklin C-SPAN, Washington Journal *LIVE*
10:03 am (est.)	Call-In 1:14 Open Phones C-SPAN, Washington Journal
11:20 am (est.)	Call-In 0:43 Diplomatic Meetings C-SPAN, Washington Journal Massimo Calabresi , *TIME* Magazine
12:06 pm (est.)	Call-In 0:03 The History of Philadelphia C-SPAN, Washington Journal

C-SPAN 2

Time	Program
08:01 am (est.)	Speech 1:25 Nurse Shortage Forum on Health Care Leadership Leah Curtin , *Curtin Calls*
09:26 am	0:22 TBA
09:49 am (est.)	Speech 0:26 Expanding the Republican Congressional Majority Virginia Young Republicans Tom Davis , R-VA
10:22 am (est.)	National Press Club Speech 0:56 Technology and Global Democratization National Press Club Robert Davis , Lycos, Inc.
11:21 am (est.)	News Conference 0:36 Republican Delegates Platform Poll American Conservative Union Donald Devine , Forbes Presidential Campaign
12:00 pm (est.)	Senate Proceeding 7:00 Senate Session U.S. Senate *The beginning and end of this live program may be earlier or later than the scheduled times.* *LIVE*

12:09 pm 0:20 - TBA -

12:30 pm 0:30 (est.) *LIVE* House Proceeding
Morning Hour
U.S. House of Representatives
The beginning and end of this live program may be earlier or later than the scheduled times.

01:00 pm 0:48 - TBA -

01:48 pm 0:28 (est.) Call-In
Benjamin Franklin
C-SPAN, Washington Journal

02:00 pm 1:45 (est.) *LIVE* House Proceeding
House Session
U.S. House of Representatives
The beginning and end of this live program may be earlier or later than the scheduled times.

03:45 pm 0:39 (est.) News Conference
Protests at the Republican Convention
R2D2 Coalition

04:24 pm 1:35 - TBA -

06:00 pm 3:00 (est.) *LIVE* House Proceeding
House Session
U.S. House of Representatives

Programs Airing Monday, 07/24/2000, not yet Scheduled

Length	Network	Program
0:00	- TBA -	Archbishop Tutu Farewell
0:00	- TBA -	Georgia Senator Appointment
8:31	- TBA -	Treasury Issues

C-SPAN Extra

Time	Program
07:00 am 6:00	TBA
01:00 pm 2:00 (est.) *LIVE*	House Committee FBI E-Mail Surveillance Program Judiciary Henry J. Hyde , R-IL Stewart Baker *The beginning and end of this live program may be earlier or later than the scheduled times.*
03:00 pm 1:00	TBA
04:00 pm 1:00 (est.) *LIVE*	House Committee Presidential Requirement Amendment Judiciary, Constitution Forrest McDonald , University of Alabama Charles Canady , R-FL *The beginning and end of this live program may be earlier or later than the scheduled times.*

C-SPAN Radio

Time	Program
07:00 am 6:00	TBA
01:00 pm 2:00 (est.) *LIVE*	House Committee FBI E-Mail Surveillance Program Judiciary Henry J. Hyde , R-IL Stewart Baker *The beginning and end of this live program may be earlier or later than the scheduled times.*
03:00 pm 1:00	TBA
04:00 pm 1:00 (est.) *LIVE*	House Committee Presidential Requirement Amendment Judiciary, Constitution Forrest McDonald , University of Alabama Charles Canady , R-FL *The beginning and end of this live program may be earlier or later than the scheduled times.*

For more information please contact schedule@c-spanarchives.org.

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
INVESTIGATIVE LAW UNIT
(THROUGH 7/28/00)

PAGES REVIEWED: 132

PAGES RELEASED: 132

EXEMPTIONS CITED: b6-1, b7C-1, b6-3 & b7C-3

NOTE: 29 Pages from this file are duplicates to pages from The Office of General Counsel's Front Office file and The Office of General Counsel/Technology Law Unit's file.

[redacted] b6-1/b7c-1

Department Of Justice
Office Legislative Affairs
Control Sheet

Date Of Document: 02/29/00
Date Received: 02/29/00
Due Date: 03/08/00

Control No.: 000301-346
ID No.: 364179

From: OMB (S.2092) (LRM-REJ280) ((106TH CONGRESS))
To: OLA

Subject:
REQUEST FOR VIEWS ON S.2092, HIGH TECH CRIME BILL

Action/Information: Signature Level: OLA

Referred To:	Date Assigned:	Action:
CRM, FBI, DAG, OLC, OPD	03/01/00	FOR YOUR INFORMATION - PREVIOUSLY CIRCULATED UNDER CONTROL NO 000228 315. CC: OLA [redacted] b6-3/b7c-3

Remarks:

Comments:

File Comments:
Primary Contact: [redacted] b6-3/b7c-3

Please take for Rec'd.

Doc #1

b6-3
b7C-3

Total Pages: 8

LRM ID: REJ280

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
Washington, D.C. 20503-0001

Tuesday, February 29, 2000

LEGISLATIVE REFERRAL MEMORANDUM

b6-3
b7C-3

TO: Legislative Liaison Officer - See Distribution below

FROM: Richard E. Green (for) Assistant Director for Legislative Reference
OMB CONTACT: [redacted]
E-Mail: [redacted]omb.eop.gov
PHONE: (202[redacted] FAX: (202[redacted]

SUBJECT: OMB Request for Views on S2092 High Tech Crime Bill

DEADLINE: Wednesday, March 8, 2000

In accordance with OMB Circular A-19, OMB requests the views of your agency on the above subject before advising on its relationship to the program of the President. Please advise us if this item will affect direct spending or receipts for purposes of the "Pay-As-You-Go" provisions of Title XIII of the Omnibus Budget Reconciliation Act of 1990.

COMMENTS: A copy of S. 2092 is attached.

Justice: Please advise of any plans to prepare a views letter on S. 2092.

DISTRIBUTION LIST

AGENCIES:
61-JUSTICE - Robert Raben - (202) 514-2141
114-STATE - Paul Rademacher - (202) 647-4463
29-DEFENSE - Samuel T. Brick Jr. - (703) 697-1305
116-TREASURY - Richard S. Carro - (202) 622-0650
25-COMMERCE - Michael A. Levitt - (202) 482-3151
36-Federal Communications Commission - Sheryl Wilkerson - (202) 418-1900
21-Central Intelligence Agency - Cynthia D. Erskine - (703) 482-8626

EOP:
Maura M. Reilly
Leanne A. Shimabukuro
Deanne E. Benos
Peter R. Swire
Lauren B. Steinfeld
Martin L. Yeung
Glenn R. Schlarman
Thomas A. Kalil
David W. Beier
James M. Kulikowski

66-3
67C-3

d H. Chase
ry Jo Sicari
Joanne Chow
Anne R. Stauffer
Charles W. Fox
Ellen J. Balis
Pamula L. Simms
Nell Lobron

tion 6412(a)(1) of such Code is ...

...by inserting "(the date of the enactment of the American Transportation Recovery Act of 2000, in the case of diesel fuel)" after "October 1, 2005" both places it appears.

(B) by inserting "(the date which is 6 months after the date of the enactment of such Act, in the case of diesel fuel) after "March 31, 2006" both places it appears, and

(C) by inserting "(the date which is 3 months after the date of the enactment of such Act, in the case of diesel fuel) after "January 1, 2006".

(4) Section 6427(l)(4) of such Code is amended by inserting "(during the 1 year period beginning on the date of the enactment of the American Transportation Recovery Act of 2000, in the case of diesel fuel)" after "September 30, 2007".

(c) EFFECTIVE DATE.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendments made by this section shall take effect on the date of the enactment of this section.

(2) DECREASE IN CRUDE OIL PRICES.—If the Secretary of Treasury determines that the average refiner acquisition costs for crude oil are equal to or less than such costs were on December 31, 1999, the amendments made by this section shall cease to take effect and the Internal Revenue Code shall be administered as if such amendments did not take effect.

By Mrs. FEINSTEIN:

S. 2091. A bill to amend the Act that authorized construction of the San Luis Unit of the Central Valley Project, California, to facilitate water transfers in the Central Valley Project; to the Committee on Energy and Natural Resources.

THE CONSTRUCTION OF THE SAN LUIS UNIT OF THE CENTRAL VALLEY PROJECTS

Mrs. FEINSTEIN. Mr. President, today I introduce a bill to amend the legislation that authorized construction of the San Luis Unit of the Central Valley Project in California. Enactment of this bill would allow water districts in the San Luis Unit of the Central Valley Project to supplement their federal water supplies with purchases of water from the State Water Project. At present, federal law prohibits the delivery of non-federal water to districts in the San Luis Unit until certain conditions are met.

The San Luis Unit is the last component created by federal law in the Central Valley Project, which is the largest Bureau of Reclamation project in the United States. Water service to districts in the San Luis Unit is often curtailed because of limitations imposed in pumping in the Sacramento-San Joaquin Delta.

It is customary for water districts in the San Luis Unit to supplement their supplies through purchases on the open market. However, current federal law prohibits them from purchasing supplies from the State Water Project and having these delivered over federal facilities. Making such deliveries is relatively easy because state and federal project conveyance facilities are interconnected. Prohibiting purchase of state water for delivery over federal facilities limits the opportunities available for San Luis Unit districts to obtain as large a supplemental supply as they would like.

Mr. President, this bill has already passed the House as H.R. 3077. It will impose no additional costs on the federal government. It contains provisions which assure that the additional water obtained by districts in the San Luis Unit cannot be used in a manner that would exacerbate current groundwater drainage problems. It is consistent with the provisions in the Central Valley Project Improvement Act that sought to encourage the exchange of water by willing sellers to provide additional supplies at reasonable cost to willing buyers. I urge the Senate to pass this bill.

By Mr. SCHUMER (for himself and Mr. KYL):

S. 2092. A bill to amend title 18, United States Code, to modify authorities relating to the use of pen registers and trap and trace devices, to modify provisions relating to fraud and related activities in connection with computers, and for other purposes; to the Committee on the Judiciary.

HIGH TECH CRIME BILL

Mr. SCHUMER. Mr. President, I rise today to introduce with my friend from Arizona, Senator KYL, a high tech crime bill aimed at combating computer crime. For the past nine months I have been discussing with law enforcement and computer crime experts how best to address the growing threat that computer crimes pose to our increasingly networked society.

Many of the best solutions are far-reaching and complex and will only be achieved through sustained and thoughtful hard work on an international level by both government and the private sector in the years ahead. There are, however, modes changes to existing laws that can be made now, which will serve as a significant first step in a much-needed effort to give law enforcement to tools they need to effectively fight cybercrime. The legislation that Senator KYL and I are introducing today will, among other things, make the following changes to existing law.

We must update our laws governing the use of what are called pen registers (which record the numbers dialed on a phone line) and trap and trace devices (which capture incoming electronic impulses that identify the originating number). These laws have become outdated and their procedures are too slow for the speed of criminals online.

Under current law, investigators must obtain a trap and trace order in each jurisdiction through which an electronic communication is made. Thus, for example, to trace on online communication between two terrorists that starts at a computer in New York, goes through a server in New Jersey, bounces off a computer in Wisconsin, and then ends in San Francisco, investigators may be forced to go successively to a court in each jurisdiction for an order permitting the trace (not to mention having to approach each provider along the way). In the recent Denial of Service attacks, hackers utilized dozens or even hundreds of "zombie" computers from which the attacks on specific sites were then launched. No doubt, these computers were located all over the country, and tracing them quickly under current law is therefore virtually impossible.

This legislation will amend current law to authorize the issuance of a single order to completely trace an online communication to its source, regardless of how many intermediate sites it passes through. Law enforcement must still meet the exact same burden to obtain such an order; the only difference is that they will not have to repeat this process over and over each time a communication passes to a new carrier in a different jurisdiction.

One deficiency of the Computer Fraud and Abuse Act, 18 U.C.C. §1030, is its requirement of proof of damages in excess of $5,000. In several cases, prosecutors have found that while computer intruders had attempted to harm computers vital to our critical infrastructures, such as telecommunications and financial services, damages of $5,000 could not be proven. Nevertheless, these intrusions pose a great risk of harm to our country and must be prosecuted, punished, and deterred.

The Schumer-Kyl bill will unambiguously permit federal jurisdiction at the outset of an unauthorized intrusion into critical infrastructure systems rather than having investigators wait for any damage assessment. Crimes that exceed the $5,000 limit will be prosecuted as felonies, while crimes below that amount will be defined as misdemeanors. The bill will also clarify that a $5,000 loss resulting from a computer attack may include the costs of responding to the offense, conducting a damage assessment, restoring a system to its original condition, and any lost revenue or costs incurred as a result of an interruption in service. The $5,000 requirement should not serve as a barrier to the prosecution of serious computer criminals who threaten our country's networks.

This legislation will also modify a directive to the sentencing commission contained in the Antiterrorism and Effective Death Penalty Act of 1996, which required a mandatory minimum sentence of six months' imprisonment for certain violations of section 1030. Computer intrusions that violate the statute vary in their severity and maliciousness. All violations should be punished, but under the current regime the mandatory imprisonment applies to some misdemeanor charges, even where the attack caused no damage. As a result, some prosecutors have declined to bring cases, knowing that the result would be mandatory imprisonment. We should insure that federal prosecutors are bringing cases under section 1030, but we also should insure that the sentences being meted out fit the crime.

most technologically savvy are juveniles who have up with computers always at ir fingertips. Unfortunately, certain juveniles are committing the most serious computer crimes and wreaking havoc on our critical infrastructures. For example, one juvenile hacker caused an airport in Worcester, Massachusetts to shut down for over six hours when its telecommunications connections were brought down. Similarly, two California teenagers broke into sensitive military computers, including those at Lawrence Livermore National Laboratory and the U.S. Air Force.

As a longer term strategy, we need to do a better job of teaching our children from a very young age that, like anywhere else, certain conduct on the Internet is wrong and illegal. But we also need to send a clear message that crimes on the Internet will have real consequences. This legislation will amend 18 U.S.C. §1030 to give federal law enforcement authorities the power to investigate and prosecute juvenile offenders of computer crimes in appropriate cases. The bill will make juveniles fifteen years of age or older who commit the most serious violations of section 1030 eligible for federal prosecution in cases where the Attorney General certifies that such prosecution is appropriate. In conjunction with the elimination of the six-month mandatory minimum, this legislation will provide a balanced, measured approach to juvenile hacking crimes.

Again, these are just the first steps that should be taken in a very long battle against cybercrime that many of us will wage for years to come. And while we fight computer crime by modifying our criminal laws, we also should seek concomitant ways to fully protect the fundamental rights of innocent individuals on the Internet.

I want to thank Senator KYL for joining me in introducing this bill. As chairman of the Subcommittee on Technology, Terrorism, and Government Information, I know that he cares deeply about these issues and I look forward to working with him on this commonsense, bipartisan legislation.•

By Mr. DOMENICI (for himself, Mr. BINGAMAN, and Mr. BAUCUS):

S. 2893. A bill to amend the Transportation Equity Act for the 21st Century to ensure that full obligation authority is provided for the Indian reservation roads program; to the Committee on Environment and Public Works.

THE TRANSPORTATION EQUITY ACT FOR THE 21ST CENTURY AND INDIAN RESERVATION ROADS

• Mr. DOMENICI. Mr. President, I am pleased today to be joined by my colleagues JEFF BINGAMAN and MAX BAUCUS in introducing legislation to preserve precious dollars allocated by the Congress and the President for construction of Indian reservation roads.

There is no doubt that the Indian reservation road system is the poorest in our nation, and every federal dollar allocated for improving this situation should be directed to our nation's Indian reservations. The lack of adequate roads and bridges is a chronic problem on Indian reservations, where unemployment averages 35 percent and more than half of American Indian live in hard poverty.

Since 1982, when my Senate amendment added Indian roads to our federal highway trust fund accounts, all funds allocated for Indian roads have been used for that purpose. In ISTEA, which preceeded the enactment of the Transportation Efficiency Act for the 21st Century (TEA-21), the Indian Reservation Roads (IRR) program reached a level of $191 million per year.

Many of us in Congress worked hard to increase this IRR funding to $225 million in the first year of TEA-21 (FY 1998), and $275 million each year thereafter, through FY 2003. Unfortunately, a little noticed provision for Federal Lands Highways, placing an "obligation limitation" on the IRR program, has resulted in the transfer of funds intended for Indian reservations to be transferred to the 50 states.

In FY 1998, the amount deducted for this transfer to states from the IRR program was $24.2 million. In FY 1999, it was $31.7 million; and in FY 2000, the obligation limitation resulted in a loss of $34.9 million that could have been used for Indian reservation road building.

In all previous enacting legislation since 1982, federal funds intended for IRR programs have been used for IRR purposes. Only in TEA-21 was this changed due to the application of the obligation limitation to Federal Lands Highways and the IRR program.

Our bill will simply exclude the IRR program from this annual deduction that has totaled, in the past three years, more than $90 million. This money, while helpful to many states, is more badly needed on Indian reservations and should be preserved for that purpose. By excluding the IRR program from this obligation limitation provision, we will be increasing federal funds for Indian roads without increasing the cost of the total program. We will be focusing the funds for Indian roads on Indian roads, as we have intended since the IRR program first became part of our federal highway trust fund in 1982.

I urge my colleagues to join us in redirecting funds intended for Indian road construction to be dedicated to that purpose.•

Mr. BINGAMAN. Mr. President, I am pleased to join today with my good friend and colleague from New Mexico, Senator DOMENICI, to introduce this bill along with Senator BAUCUS. This bill assures that our Native American communities have the funding they need for critical transportation projects. Our bill will fund the Indian Reservation Road Program for the next three years with at least $275 million per year, the full amount authorized by Congress.

Mr. President, since I came to the Senate in 1983, I've worked hard to promote economic development and create new jobs for my state of New Mexico. One thing I learned very quickly is that you can't expect to attract new industry unless you have the basic infrastructure to support residential and commercial needs. The most important infrastructure needs include transportation, power, communications, water and sewers. Without these basic services at affordable rates, opportunities to create good jobs will simply not develop.

Today our country is fortunate to have one of the strongest economies in history. Our recent advances in job creation and economic growth are accomplishments that all Americans should be proud of. Unfortunately, as many of us know, some sectors of our nation continue to lag behind the wave of economic prosperity that has swept the nation. In particular, I remain concerned about our Native American communities. Unemployment rates today in Indian Country frequently top 30, 40, and even 50 percent. Mr. President, the nation must not stand by while Indian Country is literally being left behind. Perhaps more than any other community in America, the Tribes and Alaska Native Villages suffer from inadequate infrastructure.

This year I am pleased to be working with President Clinton, Senators DASCHLE, DOMENICI, and others on a number of new programs and initiatives to help the Native American Communities enjoy the same level of economic prosperity as the rest of America. In this respect, the Tribes are no different than the rest of America—to promote their economic development basic infrastructure must first be in place. The President's initiative recognizes this fact. The bill we are introducing today addresses one element of that initiative—the need for basic transportation, including roads and transit. This bill will help promote transportation on every reservation in America by fully funding the Indian Reservation Roads Program.

First established in 1928, the Indian Reservation Roads program is one of the ways America meets its special responsibility to help Native Americans achieve self sufficiency and self determination. The goal of the Indian Reservation Roads program is to provide safe and economic means of transportation throughout Indian Country. Over the years, the program has been reauthorized and modified to help meet the Tribes' needs for basic transportation infrastructure. Most recently, the program was reauthorized for six years in 1998. The program is playing a critical role in economic development, self-determination, and employment of Native Americans in 33 states, including the Alaska Native Villages.

Currently, the reservation roads system comprises 25,700 miles of BIA- and Tribal-owned roads and 25,600 miles of state, county and local roads. There

(1) by inserting "or trap and trace device" after "pen register";

(2) by inserting ", routing, addressing," after "dialing"; and

(3) by striking "call processing" and inserting "the processing and transmitting of wire and electronic communications".

(b) ISSUANCE OF ORDERS.—

(1) IN GENERAL.—Subsection (a) of section 3123 of that title is amended to read as follows:

"(a) IN GENERAL.—(1) Upon an application made under section 3122(a)(1) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order shall, upon service of the order, apply to any entity providing wire or electronic communication service in the United States whose assistance is required to effectuate the order.

"(2) Upon an application made under section 3122(a)(2) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court

O:\ARM\ARM00.115 S.L.C.

if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.".

(2) CONTENTS OF ORDER.—Subsection (b)(1) of that section is amended—

(A) in subparagraph (A)—

(i) by inserting "or other facility" after "telephone line"; and

(ii) by inserting before the semicolon at the end "or applied"; and

(B) by striking subparagraph (C) and inserting the following new subparagraph (C):

"(C) a description of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (e)(2), the geographic limits of the order; and".

(3) NONDISCLOSURE REQUIREMENTS.—Subsection (d)(2) of that section is amended—

(A) by inserting "or other facility" after "the line"; and

(B) by striking "or who has been ordered by the court" and inserting "or applied or who is obligated by the order".

(c) EMERGENCY INSTALLATION.—Section 3125(a)(1) of that title is amended—

(1) in subparagraph (A), by striking "or" at the end;

(2) in subparagraph (B), by striking the comma at the end and inserting a semicolon; and

(3) by inserting after subparagraph (B) the following new subparagraphs:

"(C) immediate threat to the national security interests of the United States;

"(D) immediate threat to public health or safety; or

"(E) an attack on the integrity or availability of a protected computer which attack would be an offense punishable under section 1030(c)(2)(C) of this title,".

(d) DEFINITIONS.—

(1) COURT OF COMPETENT JURISDICTION.—Paragraph (2) of section 3127 of that title is

amended by striking subparagraph (A) and inserting the following new subparagraph (A):

"(A) any district court of the United States (including a magistrate judge of such a court) or any United States Court of Appeals having jurisdiction over the offense being investigated; or".

(2) PEN REGISTER.—Paragraph (3) of that section is amended—

(A) by striking "electronic or other impulses" and all that follows through "is attached" and inserting "dialing, routing, addressing, or signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"; and

(B) by inserting "or process" after "device" each place it appears.

(3) TRAP AND TRACE DEVICE.—Paragraph (4) of that section is amended—

(A) by inserting "or process" after "a device"; and

(B) by striking "of an instrument" and all that follows through the end and inserting "or other dialing, routing, addressing, and signal-

ling information relevant to identifying the source of a wire or electronic communication;".

SEC. 2. MODIFICATION OF PROVISIONS RELATING TO FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

(a) PENALTIES.—Subsection (c) of section 1030 of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in subparagraph (A)—

(i) by inserting "except as provided in subparagraphs (B) and (C)," before "a fine";

(ii) by striking "(a)(5)(C)," and inserting "(a)(5),"; and

(iii) by striking "and" at the end;

(B) in subparagraph (B)—

(i) by inserting "or an attempt to commit an offense punishable under this subparagraph," after "subsection (a)(2)," in the matter preceding clause (i); and

(ii) by adding "and" at the end; and

(C) by striking subparagraph (C) and inserting the following new subparagraph (C):

"(C) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an

offense under subsection (a)(5)(A) or (a)(5)(B), or an attempt to commit an offense punishable under this subparagraph, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

"(i) loss to one or more persons during any one-year period (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value;

"(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

"(iii) physical injury to any person;

"(iv) a threat to public health or safety; or

"(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; and";

(2) by redesignating subparagraph (B) of paragraph (3) as paragraph (4);

(3) in paragraph (3)—

(A) by striking "(A)" at the beginning; and

(B) by striking ", (a)(5)(A), (a)(5)(B),"; and

(4) in paragraph (4), as designated by paragraph (2) of this subsection, by striking "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C)," and inserting "(a)(2), (a)(3), (a)(4), (a)(6),".

(b) DEFINITIONS.—Subsection (e) of that section is amended—

(1) in paragraph (2)(B), by inserting ", including a computer located outside the United States" before the semicolon;

(2) in paragraph (7), by striking "and" at the end;

(3) by striking paragraph (8) and inserting the following new paragraph (8):

"(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information;";

(4) in paragraph (9), by striking the period at the end and inserting "; and"; and

(5) by adding at the end the following new paragraphs:

"(10) the term 'conviction' shall include an adjudication of juvenile delinquency for a violation of this section; and

"(11) the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost or cost incurred because of interruption of service.".

(c) DAMAGES IN CIVIL ACTIONS.—Subsection (g) of that section is amended in the second sentence by striking "involving damage" and all that follows through the period and inserting "of subsection (a)(5) shall be limited to loss unless such action includes one of the elements set forth in clauses (ii) through (v) of subsection (c)(2)(C).".

(d) CRIMINAL FORFEITURE.—That section is further amended by adding at the end the following new subsection:

"(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) the interest of such person in any property, whether real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, whether real or personal, constituting or derived from any proceeds that such person obtained, whether directly or indirectly, as a result of such violation.

"(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any administrative or judicial proceeding relating thereto, shall be governed by the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), except subsection (d) of that section.".

(e) CIVIL FORFEITURE.—That section, as amended by subsection (d) of this section, is further amended by adding at the end the following new subsection:

"(j)(1) The following shall be subject to forfeiture to the United States, and no property right shall exist in them:

"(A) Any property, whether real or personal, that is used or intended to be used to commit or to facilitate the commission of any violation of this section.

"(B) Any property, whether real or personal, that constitutes or is derived from proceeds traceable to any violation of this section.

O:\ARM\ARM00.115 S.L.C.

"(2) The provisions of chapter 46 of this title relating to civil forfeiture shall apply to any seizure or civil forfeiture under this subsection.".

SEC. 3. JUVENILE DELINQUENCY.

Clause (3) of the first paragraph of section 5032 of title 18, United States Code, is amended—

(1) by striking "or" before "section 1002(a)";

(2) by striking "or" before "section 924(b)"; and

(3) by inserting after ""or (h) of this title," the following: "or section 1030(a)(1), (a)(2)(B), or (a)(3) of this title, or is a felony violation of section 1030(a)(5) of this title where such violation of such section 1030(a)(5) is punishable under clauses (ii) through (v) of section 1030(c)(5)(C) of this title,".

SEC. 4. AMENDMENT TO SENTENCING GUIDELINES.

Section 805(c) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 28 U.S.C. 994 note) is amended by striking "paragraph (4) or (5)" and inserting "paragraph (4), or a felony violation of paragraph (5)(A)".

May 4, 2000

Mr. Parkinson:

Re: HIGH TECH CRIME LEGISLATION
TLU LEGISLATIVE PROPOSALS

This is to alert you to the on-going efforts of the Technology Law Unit in assisting OPCA in addressing the FBI's criminal legislative needs relating to computer and Internet investigations as well as responding to issues generated by various legislative proposals being submitted by members of Congress.

Attached are a series of documents which may be broken down into two (2) groups: 1) Amendments (with legal analysis) which the FBI supports to existing bills currently filed and under consideration, and; 2) Proposed amendments, the subject matter of which is not currently proposed bill. Some significant portions of these materials represent adaptations of proposals we support and which have been hammered out with CCIPS over the past several months. We understand from CCIPS that most of these proposals have been approved by the administration to be "shopped around" and CCIPS is generally aware of our providing technical drafting assistance and commentary to the staffs of members of Congress. This has been a time-intensive process which has absorbed significant TLU resources with regular assistance from ILU and is expected to continue until the end of the current legislative session.

b6-1
b7C-1

In addition, this is to alert you that TLU's [redacted] and [redacted] will be accompanying OPCA on Thursday, May 4, 2000 and Friday, May 5, 2000 to meet with Senator Hatch's staff and Senator DeWine's staff regarding high tech issues and FCC merger approval deadline issues (S.467) respectively.

Patrick W. Kelley
Deputy General Counsel

1 - Mr. Collingwood
1 - [redacted]
1 - Mr. Steele
1 - [redacted]

1 - [redacted]
1 - [redacted]
1 - [redacted]
1 - [redacted]

1 - [redacted]
1 - 66F-HQ-C1299934

b6-1
b7C-1

Doc #2

PRIORITY OF MATTERS CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION.

1) Support funding for Technical Support Center and Regional Computer Forensic Laboratories. (Hatch)

2) "Tweaking" of language in the amending Pen Register/Trap and Trace Statute. (Kyl/Schumer)

3) "Tweaking" of language amending the Computer Fraud Statute. (Kyl/Schumer and Hatch)

4) Oppose Expansion of Secret Service 18 U.S.C. §1030 jurisdiction. (Hatch)

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

Support funding for Technical Support Center and Regional Computer Forensic Laboratories

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

1. "Support funding for Technical Support Center and Regional Computer Forensic Laboratories"

Support For Direct Funding to the FBI for the National Cyber-Crime Technical Support Center

The FBI strongly supports without reservation the provisions of section 109(a) of S.2448 as a necessary and critical element in United States' strategy to combat cyber-crime on a national and international level. The absence of adequate technical resources dedicated to the assistance of law enforcement in this arena undermines daily the investigative efforts of federal, state and local law enforcement officers dedicated to addressing the most troubling aspects of computers and the Internet such as child sexual exploitation, the dissemination of child pornography, the wholesale theft of intellectual property, the theft and disclosure of valuable trade secrets as well as countless more traditional crimes now being facilitated by the use of computers. The FBI's existing technical expertise, established with the FBI Laboratory Divisions's Engineering Research Facility, demonstrates the prudence in providing funding dedicated for these expressed purposes directly with the Director of the FBI as the most effective means of ensuring that such a facility is constructed and made operational with the least delay possible. Senate Bill 2448's approach is necessary, prudent and expeditious.

Support for Direct Funding to the FBI for the Creation of Regional Computer Forensic Laboratories

The FBI also supports without reservation the provisions of section 109(b) of S.2448 authorizing direct funding to the FBI for the express purpose of creating up to ten (10) Regional Computer Forensic Laboratories (RCFLs).

The FBI notes that, by separating funding for RCFLs under section 109(b) of S.2448 from State funding for task forces and other DOJ controlled investigative initiatives under 109(c), the bill implicitly acknowledges the difference between a true computer forensics capability which is and should be an objective, scientific function and a computer investigative capability[1], and have appropriately chosen to lodge responsibility for the former with the FBI through its laboratory division.

It is well known that the FBI Laboratory Division was instrumental in the development and realization of a Regional Computer Forensic Laboratory in San Diego, California at which federal, state and local law enforcement officers work side by side sharing both expertise and expensive equipment and software vital to the forensic recovery of often critical criminal evidence from computers and other digital media. The FBI Laboratory utilized its own financial resources to make the San Diego RCFL a reality and is providing extensive computer forensic training to state and local officers of that facility both at the FBI Academy and through computer industry recognized training programs. The FBI Laboratory Division now has some twenty (20) years experience in the science of computer forensics through its Computer Analysis Response Team (CART). With CART scheduled to expand from its current forensic complement of over 120 examiners to over 300 by the beginning of 2002 (which will continue to secure its place as the single largest computer forensic entity in the world), it only makes good sense to harness the FBI's expertise and knowledge of scientific method and forensic "best practices" as the means of jump starting a legitimate state and local computer forensic capability. The key to the success of the San Diego RCFL will be the key to success for future RCFLs, namely the ability to move quickly with a minimum of administrative expense, overhead or red tape. S.2448's direct funding appropriation make this possibility a reality.

For these and many other reasons, the FBI strongly supports the allocation of direct funding for RCFLs to the FBI.

---

[1]A computer investigative capability typically requires specially trained officers who are versed in Internet culture, Internet-based ponzi and othe fraud schemes as well as Internet chat vernacular enabling them to go on-line undercover to detect and investigate criminal behavior. In comparison, the focus of a computer forensics capability is the recovery, extraction, interpretation and stabilization of digital evidence, usually from digital storage media such as a computer hard drive seized as a result of a computer investigation. Computer forensic examiners typically are required to possess and master a far more detailed knowledge of electronics, computer hardware assembly and operation and software programing and operation than would be necessary for a computer investigator. A computer forensic facility is more detached from heat of the investigation and employs scientifically proven or accepted methodologies to recover either inculpatory or exculpatory evidence from a digital medium.

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

2. "Tweaking" of language in the amending Pen Register/Trap and Trace Statute. (Kyl/Schumer)

AMENDMENTS TO THE PEN REGISTER AND TRAP & TRACE STATUTE

It is suggested that the last sentence of the proposed modification of 18 U.S.C. § 3122(a) (and its legislative history) be changed to make clear that service of the new single, nation-wide court order is not required upon all providers in the communication chain if a single provider has access to all transmission data. The suggested change is:

"~~The order shall~~ Such order shall, upon service of the order, apply to any entity providing wire or electronic communications service in the United States whose assistance ~~is required to effectuate the order~~ may facilitate the execution of the order."

It is also suggested that the proposed revision to 3123 subsection (b) (1), new subparagraph (C) be changed for the reasons stated below in the proposed legislative history:

"(C) a description of --

(i) the technical nature of the communications to which the order applies, such as ~~including~~ the number or other identifier"

PROPOSED LEGISLATIVE HISTORY

Existing Subsection (C) is intended to require the identification of the "facility" to which the pen register or trap and trace is applied. Historically this was accomplished by identifying the telephone number of the targeted telephone, and if known the physical location of that telephone. With the increase in electronic communications via e-mail, chat sessions, instant Messaging, or telenet sessions, it may not always be possible to identify a static "facility." In cases of dynamic addressing of Internet accounts and telenet sessions for example, it is difficult to describe the facility through a static number. To address this, the statute should permit the applicants to describe the technical nature of the communications as a means of further identifying the facility to which the order applies. Examples might include the computer protocol or computer language utilized, or any dynamically assigned message identification number or code or part thereof.

The bill also inserts "routing, addressing" into the phrase "dialing and signaling information" in section 3121(c) and other provisions of the statute. The term "signaling" has historically been given an expansive reading to include, in the electronic communications world (e.g., e-mail), much of what would be "routing and addressing" and then some. It is stressed that the insertion and existence of "routing, addressing" into the statute is not intended to limit the interpretation of the term "signaling."

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

3. "Tweaking" of language amending the Computer Fraud and Abuse Act.

SUGGESTED ADDITIONAL AMENDMENTS TO THE COMPUTER FRAUD AND ABUSE ACT.

Counting Prior State Computer Crime Offenses:

A new § 1030(e)(10) would define conviction to include prior Federal juvenile adjudications for violations of § 1030. Given that the majority of States now have unauthorized computer access or similar computer crime statutes[2], it is suggested that the proposed new definition of conviction be further expanded to include prior State computer convictions. The

---

[2] Some 45 States have enacted statutes prohibiting, to varying degree, computer crime: AL Computer Crime Act, Code of Alabama, Sections 13A-8-100 to 13A-8-103; AK Statutes, Sections 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990; AZ Revised Statues Annotated, Sections 13-2301(E), 13-2316; CA Penal Code, Section 502; CO Revised Statutes, Sections 18-5.5-101, 18-5.5-102; CT General Statutes, Sections 53a-250 to 53a-261, 52-570b; DE Code Annotated, Title 11, Sections 931-938; FL Computer Crimes Act, Florida Statutes Annotated, Sections 815.01 to 815.07; GA Computer Systems Protection Act, Georgia Codes Annotated, Sections 16-9-90 to 16-9-95; HI Revised Statutes, Sections 708-890 to 780-896; ID Code, Title 18, Chapter 22, Sections 18-2201, 18-2202; IL Annotated Statutes (Criminal Code), Sections 15-1, 16-9; IN Code, Sections 35-43-1-4, 35-43-2-3; IO Statutes, Sections 716A.1 to 716A.16; KS Statutes Annotated, Section 21-3755; KY Revised Statutes, Sections 434.840 to 434.860; LA Revised Statutes, Title 14, Subpart D. Computer Related Crimes, Sections 73.1 to 73.5; ME Revised Statutes Annotated, Chapter 15, Title 17-A, Section 357; MD Annotated Code, Article 27, Sections 45A and 146; MA General Laws, Chapter 266, Section 30; MI Statutes Annottated, Section 28.529(1)-(7); MN Statutes (Criminal Code), Sections 609.87 to 609.89; MI Code Annotated, Sections 97-45-1 to 97-45-13; MS Revised Statutes, Sections 569.093 to 569.099; MT Code Annotated, Sections 45-2-101, 45-6-310, 45-6-311; NE Revised Statutes, Article 13(p) Computers, Sections 28-1343 to 28-1348; NV Revised Statutes, Sections 205.473 to 205.477; NH Revised Statutes Annotated, Sections 638:16 to 638:19; NJ Statutes, Title 2C, Chapter 20, Sections 2C:20-1, 2C:20-23 to 2C:20-34, and Title 2A, Sections 2A:38A-1 to 2A:38A-3; NM Statutes Annotated, Criminal Offenses, Computer Crimes Act, Sections 30-16A-1 to 30-16A-4; NY Penal Law, Sections 155.00, 156.00 to 156.50, 165.15 subdiv. 10, 170.00, 175.00 NC General Statutes, Sections 14-453 to 14-457; ND Century Code, Sections 12.1-06.1-01 subsection 3, 12.1-06.1-08; OH Revised Code Annotated, Sections 2901.01, 2913.01, 2913.04, 2913.81; OK Computer Crimes Act, Oklahoma Session Laws, Title 21, Sections 1951-1956; OR Revised Statutes, Sections 164.125, 164.377; PA Consolidated Statutes Annotated, Section 3933; RI General Laws (Criminal Offenses), Sections 11-52-1 to 11-52-5 SC Code of Laws, Sections 16-16-10 to 16-16-40; SD Codified Laws, Sections 43-43B-1 to 43-43B-8; TN Code Annotated, Computer Crimes Act, Sections 39-3-1401 to 39-3-1406; TX Codes Annotated, Title 7, Chapter 33, Sections 33.01 to 33.05; UT Computer Fraud Act, Utah Code Annotated, Sections 76-6-701 to 76-6-704; VA Computer Crime Act, Code of Virginia, Sections 18.2-152.1 to 18.2-152.14; WA Revised Code Annotated, Sections 9A.48.100, 9A.52.010, 9A.52.110 to 9A.52.130 WI Statutes Annotated. Section 943.70; WY Statutes, Sections 6-3-501 to 6-3-505.

suggested additional language to the proposed bills' § 1030(e)(10) version would be:

> "; and
> (B) a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer."

Given the fact that most section 1030 offenders are juveniles and statistically more likely to first receive State juvenile adjudications, it is further recommended that the provision go even further than that outline above by including prior State juvenile adjudications.

Expanding the Definition of "loss" to Include Preventative Reconfiguration:

Another recommendation for the Hatch Bill is that the proposed definition of "loss" in Section 1030(e)(11) be made clearer to include the cost of plugging holes in computer defenses as a means of preventing future attacks---so called "preventative re-configuration/reprogramming." The new language could read:

> "(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, implementation of responsive security measures or reconfiguration reasonably calculated to prevent future damage, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;"

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

4. Oppose Expansion of Secret Service 18 U.S.C. §1030 jurisdiction.

EXECUTIVE SUMMARY

Basis of Opposition to Amendment to Grant Concurrent Jurisdiction to the United States Secret Service in Section 1030 Offenses.

The proposed amendment to section 1030(d) of Title 18 would grant concurrent jurisdiction to the United States Secret Service (USSS) to investigate all crimes found in Section 1030.

In 1996, Congress specifically limited the Secret Service's authority to investigate crimes under 18 U.S.C. § 1030 to only those offenses under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The Senate Report accompanying the 1996 amendment explained that:

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

S. Rep. No. 357, 104th Cong., 2d Sess. 13 (1996).

Inherent in the 1996 changes was the recognition that the statute was being amended to reflect the respective investigative jurisdictional limits existing at that time. It was clear at that time, that the jurisdiction of the Secret Service, found at 18 U.S.C. § 3056, did not encompass the types of offenses described in Section 1030 (a)(1), (a)(2)(C), or (a)(7).[3] Given that there have been no additional grants of investigative jurisdiction to the USSS since that amendment, the current proposal to grant jurisdiction to the USSS is at best questionable. The theft of National Security information which is the type of information Section 1030(a)(1) was intended to address has never been the subject of USSS jurisdiction, nor should it be. In addition, the types of crimes contemplated by 1030(a)(2)(C) and (a)(7), as recognized by the legislative

---

[3] "Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates –

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, credit and debit card frauds, and false identification documents or devices; except that the authority conferred by this paragraph shall be exercised subject tot he agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

history, have traditionally been investigations solely in the province of the FBI.

The 1996 provision is an explicit effort by Congress to address the criminal offenses at issue through a division of labor primarily determined by investigative responsibility and expertise. Any reversion to the pre-1996 jurisdictional provisions raises serious issues and concerns about the utilization of resources. Concurrent jurisdiction will result in a duplication of efforts that will waste resources and will encourage independent investigations by separate agencies at the expense of coordinated joint efforts.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION.

1. Cable Communications Act amendment.

EXECUTIVE SUMMARY
Cable Communications Policy Act Amendment

The Cable Communications Policy Act, passed in 1984 to regulate various aspects of the cable television industry, did not take into account the changes in technology that have occurred over the last fifteen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. This amendment clarifies that when a cable company acts as a telephone company or an Internet service provider, it must comply with the laws governing the interception and disclosure of wire and electronic communications just like any other telephone company or Internet service provider.

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER V-A--CABLE COMMUNICATIONS
PART IV--MISCELLANEOUS PROVISIONS

Section 551. Protection of subscriber privacy

(a) Notice to subscriber regarding personally identifiable information; definitions

(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of--

(A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;

(B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

(C) the period during which such information will be maintained by the cable operator;

(D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and

(E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h) of this section--

(A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;

(B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and

(C) the term "cable operator" includes, in addition to persons within the definition of cable operator in section 522 of this title, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.

(b) Collection of personally identifiable information using cable system

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to--

(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or

(B) detect unauthorized reception of cable communications.

(c) Disclosure of personally identifiable information

(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is--

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; ~~or~~

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if--

(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and

(ii) the disclosure does not reveal, directly or indirectly, the--

(I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or

(II) the nature of any transaction made by the subscriber over the cable system of the cable operator; or

(D) required under chapters 119, 121, or 206 of title 18, United States Code. Such disclosure shall not include records revealing customer cable television viewing activity. For purposes of this section, "customer cable television viewing activity" shall mean the cable customer viewing habits of operator-selected, pre-

scheduled video and audio presentations.

(d) Subscriber access to information

A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) Destruction of information

A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) of this section or pursuant to a court order.

(f) Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy

(1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(B) punitive damages; and

(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

(3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) Regulation by States or franchising authorities

Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) Disclosure of information to governmental entity pursuant to court order

Except as provided in subsection (c)(2)(D), a ~~A~~ governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order--

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

PROPOSED LEGISLATIVE HISTORY FOR AMENDMENTS TO THE CABLE COMMUNICATIONS POLICY ACT

The Cable Communications Policy Act currently establishes two different sets of rules regarding privacy protection and disclosure to law enforcement: one governing cable service ("Cable Act") (47 U.S.C. §551), and the other applying to the use of telephone service and Internet access, (the wiretap statute (18 U.S.C. §2510 et seq.), the Electronic Communications Policy Act ("ECPA") (18 U.S.C. §2701 et seq.), and the pen register and trap and trace statute (18 U.S.C. §3121 et seq.). Yet today, unlike in 1984 when Congress passed the Cable Communications Policy Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. The rules governing law enforcement access to the records of communication service providers' customers, however, should not depend on whether the customer has chosen to use a cable company or a more traditional type of provider for his telephone or Internet service. Congress believes that cable companies offering such services should comply with court orders and other legal process permitted under the wiretap statute, ECPA, and the pen register and trap and trace statute with respect to their telephone and Internet customers.

In recent years, however, cable companies have increasingly balked at complying with such process, noting the seeming inconsistency of these statutes with their duty of nondisclosure (except under stringent limits) under the Cable Communications Policy Act. See In re Application of United States, 36 F. Supp. 2d __ (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) against cable company providing Internet service). These complications have at times delayed or frustrated investigations.

In addition, section 551 is flawed because it permits law enforcement to obtain information only when that information constitutes evidence of an offense. In some cases, however, the information sought from a service provider is not evidence of a crime, even though it helps to solve one. For example, law enforcement officials may try to arrest a fugitive who is accessing his e-mail account from a remote location, and they need to obtain information from

the cable company that shows from what location he is accessing that account. Moreover, whether law enforcement can obtain a court order to obtain such information should not depend on whether the fugitive has chosen to connect to the Internet using a cable company instead of a traditional Internet service provider.

Accordingly, the amendment inserts a new subsection 551(c)(2)(D) to confirm that cable companies, like other providers, remain subject to ECPA, the wiretap statute, and the trap and trace statute with respect to the provision of telephone and Internet services, notwithstanding section 551. The definition of "customer cable television viewing activity" is intended to exclude from disclosure under chapters 119, 121, or 206 of title 18 of the United States Code traditional cable and broadcast television video/audio presentations Unlike Internet video presentations, the subject content and timing of which are selected by the cable customer, the selection and timing of television presentations are controlled by the operator. The disclosure exclusion is not intended to encompass or prohibit the disclosure by an operator of records or information relating to television presentations which are re-transmitted through the Internet. Records relating to such re-transmissions would be treated like all other Internet-related records under chapters 119, 121, or 206 of title 18. The amendment, however, is intended to preserve the Cable Act's primacy with respect to records revealing what ordinary cable television programing a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can compel disclosure under ECPA only those customer records relating to Internet service.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

2. Privacy Protection Act amendment

EXECUTIVE SUMMARY

Necessary Amendments to the Privacy Protection Act - 42 U.S.C. § 2000aa, *et seq.*

The Privacy Protection Act (PPA) prohibits law enforcement from searching for or seizing work product materials or documentary materials possessed by a person in connection with a purpose to disseminate them to the public in a newspaper, book, broadcast, or other similar form of public communication. Originally adopted to prevent the search of third party news-gathers in traditional media (e.g., newspaper press rooms, tv editor offices), the PPA has generated unforseen obstacles for law enforcement when applied to the search of a criminal's personal computers if the computers coincidentally are being used for web site publishing. A scenario frequently encountered by law enforcement involves the seizure of a computer used to disseminate child pornography which may coincidentally also control the e-mail and/or websites of the suspect and third parties. Because of the size of modern personal computer hard drives today, most computers cannot effectively be searched on scene, but are usually seized first, then searched later in a computer forensic environment as expressly provided for by a magistrate issuing the warrant. Unfortunately, such a practice creates a dilemma for investigators who may learn later during the examination process that potential third party news gatherer material may exist on the computer system. The realization may be too late as the PPA prohibits both search and seizure of such material.

Amendments detailed herein would carve out a reasonable exception to the Act when the search or seizure of work product materials or documentary materials is "incidental to" the search or seizure of other evidence relevant to a crime. Thus, the seizure of a computer hard drive of non-defendant third party for evidence of child pornography would not be prohibited merely because the same hard drive contained work product or other documentary material prohibited by the PPA.

[redline strikeout version of amendments to the Privacy Protection Act]

UNITED STATES CODE ANNOTATED
TITLE 42. THE PUBLIC HEALTH AND WELFARE
CHAPTER 21A--PRIVACY PROTECTION
SUBCHAPTER I--FIRST AMENDMENT PRIVACY PROTECTION
PART A--UNLAWFUL ACTS

Section 2000aa. Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses

(a) Work product materials

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275 or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18); ~~or~~

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being~~.~~; or

(3) the seizure or examination of work product materials is incidental to the execution of

an otherwise lawful search or seizure.

(b) Other documents

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275, or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18);

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being;

(3) there is reason to believe that the giving of notice pursuant to a subpoena duces tecum would result in the destruction, alteration, or concealment of such materials; ~~or~~

(4) such materials have not been produced in response to a court order directing compliance with a subpoena duces tecum, and--

(A) all appellate remedies have been exhausted; or

(B) there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice~~;~~ or

(5) the seizure or examination of documentary materials is incidental to the execution of an otherwise lawful search or seizure.

(c) Objections to court ordered subpoenas; affidavits

In the event a search warrant is sought pursuant to paragraph (4)(B) of subsection (b) of this section, the person possessing the materials shall be afforded adequate opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure.

PROPOSED LEGISLATIVE HISTORY FOR
AMENDMENTS TO THE PRIVACY PROTECTION ACT

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. § 2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any *work product materials*" or any "*documentary materials* ... possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa(a), (b). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public, except if the materials constitute contraband or the fruits or instrumentalities of crime. Id. § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. Id. § 2000aa-7(a). Thus, other than for the exceptions, the PPA effectively imposes a "no-search" rule on work product materials and a "subpoena-first" rule on documentary materials held by third parties who plan to use them to communicate to the public. Although the statute appears reasonable on its face, its application in the current electronic environment has inadvertently shielded criminal activities from legitimate law enforcement investigations, such efforts to arrest and prosecute those who distribute child pornography over the Internet.

(a) Intent of the PPA

Congress passed the PPA in response to the Supreme Court's decision in Zurcher v. Stanford Daily, 436 U.S. 537 (1978). In Zurcher, the Supreme Court upheld a police search, pursuant to a valid search warrant, of the offices of The Stanford Daily newspaper for photographs taken at the scene of a crime. The Court rejected the newspaper's claim that search warrants could not be used to recover evidence from those engaging in First Amendment-protected activities. Id. at 565-567. The Court also held that law enforcement officers could use search warrants to recover evidence from innocent third parties. Id. at 555 ("state's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not"). The Court concluded, therefore, that "the critical element in a reasonable search is not that the owner of the property is suspected of a crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." Id. at 556.

In response to the Court's ruling, Congress passed the PPA. Congress intended to restrict searches for mere evidence of crime held by *innocent third parties* who were engaged in First Amendment-protected activities — evidence that law enforcement officials might otherwise obtain through less intrusive means, such as by issuing a subpoena. The purpose of restricting law enforcement in this fashion, of course, was to protect the confidentiality of non-evidentiary files also held by this special group of innocent third parties — both the drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) which they never intended to publish. Thus, the PPA protects an author or publisher (like The Stanford Daily) — who is not a suspect in the investigation — from law enforcement attempts to search

through his or her work product or documentary materials in order to find and seize evidence. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third parties to find and produce it themselves. This goal of Congress remains unchanged, and our amendments do not alter this protection for innocent third parties.

Congress never intended, however, to protect criminals from court-authorized searches, and the legislative history to the PPA is replete with statements to this effect. For example, the Senate Judiciary Committee Report stated that the purpose of the PPA is to "limit searches for materials held by persons involved in First Amendment activities *who are themselves not suspected* of participation in the criminal activity for which the materials are sought." S. Rep. No. 96-874, 96th Cong., 2d Sess. 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3957 (emphasis added). Moreover, the Committee Report stated that the intention in enacting the PPA was "not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation." Id. Indeed, the language of the statute itself allows searches and seizures of any person who "has committed or is committing the criminal offense to which the materials relate." 42 U.S.C.A. § 2000aa(a)(1), (b)(1). Plainly, Congress had no desire to inhibit law enforcement investigators that need to search the premises of a suspected wrongdoer.

(b) The problem of commingling of protected documents and evidence

Because Congress enacted this statute before the widespread proliferation of computers, it could not fully consider the problem raised by the commingling of protected information and contraband. Although commingling can, of course, occur with paper records — for example, if a reporter engaging in tax fraud placed a copy of the fraudulent tax return in a filing cabinet with his or her work-related notes — such commingling never presented a significant problem for two reasons. First, the statute applied only to members of the traditional media, a limited group not usually associated with committing crimes. Second, when searching for paper records, investigators can generally examine records on site and then seize only those records that are the subject of their warrant. Thus, investigators can avoid violating the PPA by not "searching for" or "seizing" any protected material since they do not need to carry away anything but the object of their search.[4]

With the widespread use of computers and the Internet, however, both of these limiting factors have disappeared. First, every computer user has become a potential publisher. For example, a single computer can provide (1) an electronic "bulletin board" for the posting of news items by individuals using the Internet; (2) user accounts where private individuals can store drafts of news items that they intend to post on the "bulletin board"; and (3) a website from

---

[4] Of course, investigators may briefly isolate or possess protected material during the execution of the warrant, but such possession occurs during the execution of every search warrant and does not constitute a seizure.

which anyone with access to the Internet could view or download child pornography. Although the second category of data arguably constitutes "work product" under the PPA,[5] law enforcement officials plainly have the duty to search for and seize the third category of data.

Second, potential liability under the PPA may arise for law enforcement officials in such a scenario because it has become both unreasonable and impractical, and in some instances technically impossible to search for and seize the contraband without simultaneously seizing protected material. In the new electronic environment, where computer systems with gigabytes of storage have become ubiquitous, law enforcement agents generally cannot extract legally seizable evidence from commingled protected material without actually seizing, at least temporarily, those protected materials, or, perhaps more intrusively, without moving into and occupying the search premises for extended durations. Because of the volume of data to be searched or because of technical concerns (e.g. encryption), law enforcement agents must very often remove the seized computer or an exact copy of all the data to a laboratory for analysis.

Moreover, liability may attach in such cases because the prohibition on searching for or seizing materials is stated in the disjunctive: violations may lie *either* for searching for *or* seizing such materials. Thus even a temporary seizure or examination may result in liability, despite the fact that such a PPA violation lies far outside the scope of the issues raised by the Zurcher decision. Zurcher involved a search of a newspaper office, and the warrant was drawn to intentionally seize photographs that had been made in contemplation of publication. The PPA, designed to address the Zurcher decision, accordingly should deter law enforcement from intentionally *searching for* evidentiary materials in the possession of innocent third parties engaged in information dissemination. But making unlawful the reasonable but incidental seizure of PPA-protected materials pursuant to an otherwise lawful search or seizure carries no similar deterrent effect, and it contravenes the clearly stated intent of Congress to neither shield criminals nor unduly hinder law enforcement efforts.

(c) Problems faced by law enforcement

The potential — and unpredictable — liability inadvertently created by the PPA has inhibited the investigation and prosecution of crimes committed using computers. For example, individuals have used computers to distribute child pornography, copyrighted software, and stolen credit card numbers over ordinary phone lines and the Internet. Some of these individuals have attempted to use the PPA to shield their illegal activities by intentionally storing PPA-protected materials on the same storage devices that they use for their illegal activities. Indeed, law enforcement agents have encountered individuals using computers for illegal activities that have posted the following message on their sign-on screens:

---

[5] No court has yet held that an electronic message, posted for viewing by the general public by way of a Bulletin Board System or the Internet, constitutes a "similar form of public communication" to newspapers, books, and broadcasts under the PPA. Although the instant amendments to the PPA do not opine on this subject, a court might make this ruling if presented with the right facts.

NOTICE TO LAW ENFORCEMENT AGENTS:

> The owners and users of this system are exercising First Amendment Rights. . . . Some material on this system is in preparation for public dissemination and is "work product material" protected under the First Amendment Privacy Protection Act of 1980 . . . . Each and every person who has such "work product material" stored on this system is entitled to recover at least minimum damages of $1000 *plus all legal expenses* . . . . While the agency you work for *might* pay your legal fees and judgments against you, why take chances?

The language "[s]ome material on this system" is extremely significant. It is seldom the case that a computer is used solely for illegal purposes such as the distribution of contraband. Were this the case, the computer and the evidence it contains could be seized without regard to the PPA, since contraband is specifically excluded from the definitions of work product and documentary materials. 42 U.S.C. § 2000aa-7(a) (defining "documentary materials"); 42 U.S.C. § 2000aa-7(b) (defining "work product materials"). In most cases, only certain portions of a website or electronic bulletin board will be set aside for illegal activities, while other portions are used for completely legal activities such as the legitimate distribution of information. As the quoted language makes clear, however, criminals are well aware that under the PPA, protected materials can be used to shield contraband from search and seizure. Congress, of course, never intended to shield contraband when it enacted the PPA.

Moreover, in addition to exposing law enforcement to unintended liability, the PPA, as it stands, creates unnecessary problems during the execution of warrants, problems that potentially harm the health and safety of the public. In 1999, for example, Special Agents of the Federal Bureau of Investigation uncovered a system of computers used to provide child pornography to anyone with access to the Internet. These computers, however, also provided Internet accounts to third parties, many of whom did not know about the illegal activities of the computers' operators. These unrelated accounts may have contained material protected by the PPA. The investigators determined that it would be impossible to search the computers on site while at the same time allowing the computers to continue to operate. Thus, in an effort to reduce their potential liability under the PPA for seizing the third party accounts, the investigators decided to obtain a search warrant authorizing them only to *copy* the computers' stored data and allow the computers to continue to operate. This, of course, had the effect of allowing the child pornography to remain accessible to the public — and possibly even allowing the pornographers or their confederates to copy the images to an unknown computer — while computer experts reviewed the data to segregate the illegal files. Congress never intended to hamper law enforcement efforts in this way.

(d) The solution

While the PPA must be amended so that it does not shield child pornographers,

copyright infringers, and other criminals, such amendments should not inhibit those activities that the PPA was designed to protect. Indeed, the importance of protecting the confidentiality of these sensitive materials remains as great today as it has ever been. Thus, the law should limit the intrusiveness of government searches but should not unnecessarily hinder law enforcement's efforts to enforce the criminal laws. The language of this bill achieves this delicate balance between important values.

The bill's new provisions, Title 42, United States Code, sections 2000aa(a)(3) and 2000aa(b)(5), make it clear that law enforcement agents may still search for or seize contraband, instrumentalities, and evidence not protected by the PPA, even if work product or documentary material may incidentally be examined or seized during a search. It is important to note, however, that where an innocent third party possesses the items sought, and if the items sought are commingled with work product or documentary materials, existing regulations already require investigators to avoid using a search warrant or subpoena where less intrusive means are appropriate. See, e.g., 28 C.F.R. 50.10 (requiring Justice Department officials to use all other means available to obtain information before issuing subpoena to member of the news media); 28 C.F.R. §59.4(a) and 28 C.F.R. §59.4(c)(1)(11) (in determining whether to use a warrant or subpoena to obtain documentary materials, an attorney for the government should consider whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect). Thus, even though the PPA would not restrict such incidental seizures, the Committee believes that government agents will need to consider what method is proper for obtaining the evidence based upon the facts of the case at hand.

Although these amendments to the PPA address the problem of incidental searches or seizures, these changes do not in any way alter the statute's effect in cases like Zurcher. The law enforcement officials who searched The Stanford Daily — which was not involved in any criminal activity — sought the very documentary materials that the PPA now protects. These materials, therefore, were not "incidental" to the search, and they therefore would not meet the exception found in the new amendments. Thus, even under the new law, when law enforcement agents encounter a situation like that in the Zurcher case, they will still have to use a subpoena as the original PPA directed.

But in other cases, where the search is "otherwise lawful" (i.e. the object of the search is something other than "work product" or "documentary" materials), these amendments to the PPA will ensure that investigators can carry out their duties, even when PPA-protected materials may be commingled with seizable ones. The amendments' use of the term "incidental" clearly prohibits situations in which protected materials are the object of the search. The term "incidental," which appears in other statutes (see, e.g., 18 U.S.C. §2510(17)), means something which is "occurring or likely to occur at the same time or as a consequence."[6] Accordingly, in order to be "incidental" within the intent of this provision, any search or seizure of protected materials would have to be a concomitant consequence of a search for materials not protected by

---

[6] The American Heritage Dictionary, Second College Edition (1989).

the PPA.[7]

Additionally, of course, the link between the incidental items and the lawful object of the search or seizure must be reasonable on the facts of the case. This requirement that such a search be reasonable is directly analogous to the Fourth Amendment requirement of reasonableness both in the scope of a search warrant and in its execution. See O'Connor v. Ortega, 480 U.S. 709, 726 (1987); United States v. Henson, 848 F.2d 1374 (6th Cir. 1988); United States v. Tamura, 694 F.2d 591 (9th Cir. 1982). Cases that have nothing to do with the PPA have caused courts to wrestle with whether, under all the facts and circumstances, seizing certain incidental materials was sufficiently reasonable to meet the Fourth Amendment standard. Thus, the amendments do not, by any means, invite law enforcement to use "an otherwise lawful" search as a pretext for an unreasonable rummaging of other documents — whether protected by the PPA or not. On the contrary, this new exception to the PPA will allow courts to apply existing and well-established Fourth Amendment jurisprudence in analyzing the analogous question of whether any incidental search or seizure of PPA-protected materials has been reasonable under the circumstances.

[7] This provision does not, of course, require that the incidental seizure of protected materials be inadvertent; law enforcement officers may knowingly seize protected materials where such seizure is incidental to a lawful search.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

4. Clean Hands Exception to the Statutory Suppression of Intercepted Communications.

EXECUTIVE SUMMARY

Amendments Creating a "Clean Hands" Exception to Provisions Statutorily Mandating the Suppression of Illegally Intercepted Communications.

The accompanying amendments would create a "clean hands" exception to the statutory suppression mandates of 18 U.S.C. §2515 governing the use and introduction of illegally intercepted wire or oral communications. The proposal would allow for the use in a criminal investigation and the introduction into evidence in criminal matters of communications otherwise illegally intercepted by persons other than law enforcement, ONLY if law enforcement was neither directly or indirectly involved in its acquisition. Not unlike the rationale supporting the "good faith" exception to the Fourth Amendment's exclusionary remedies, implicit in the proposed amendment is the determination that the truth-finding functions of the criminal process are paramount when there is little or no law enforcement deterrence effect achievable. In contrast to existing law which prohibits all use, the proposed amendment would allow the introduction of such evidence both when it is inculpatory or exculpatory in nature.

"CLEAN HANDS" EXCEPTION TO STATUTORY EXCLUSIONARY RULE

(Exclusive of Other Substantive Amendments)

Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

(a) Except as provided in subsection (b), ~~Whenever~~ whenever any wire, or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

(b) Subsection (a) shall not apply to the disclosure or use, in a criminal investigation, proceeding, hearing or trial, or before a grand jury, of the contents of a communication, or evidence derived therefrom—

(1) intercepted by a person not acting under color of law, provided that the party seeking to disclose or use the contents did not participate directly or indirectly in the interception, or

(2) against a person alleged to have intercepted the communication, or participated in its interception, in violation of this chapter.

Section 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter (or under circumstances described in section 2515(b)), has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter (or under circumstances described in section 2515(b)), has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political

subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

Section 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing

probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual

operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (8)(d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections

(1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court,

department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval;

except that no suppression may be ordered under the circumstances described in section 2515(b). Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for non-constitutional violations of this chapter involving such communications.

"Clean Hands" Exception Proposed Legislative History

Inapplicability of 18 U.S.C. §2515 statutory exclusion and non-use of certain "clean hands" good faith disclosures

This proposed change makes a carefully limited amendment of 18 U.S.C. §2515, the statutory exclusionary rule for violations of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, so as clearly to exempt two situations: (1) those in which private individuals illegally intercept or record a communication, but the recording later comes into the possession of a party in a criminal trial, who then wishes of introduce it; and (2) those in which an individual violates chapter 119 (*e.g.*, by engaging in an illegal wiretap) and the government thereafter seeks of use the communication to prosecute that violator.

At present, appellate decisions are in apparent conflict over whether section 2515 precludes the use of communications in the first category described above. Under one possible interpretation of section 2515, if a private individual consensually records a conversation in aid of an illegal activity, or illegally records a conversation between other parties without their consent, the contents of such recordings are not admissible in a criminal trial or hearing even if the government had no role in having the evidence recorded and only acquired it, through lawful means, at a later date. This situation occurs because, under 18 U.S.C. §2511(2)(d), a consenting party, not acting under color of law, may record only if the recording is for a non-criminal or non-tortious purpose. Thus, if the payer of a bribe secretly records the transaction in which he or she pays the bribe of an official, and the government later obtains the recording and seeks of use it against the official of prove the bribe, section 2515 arguably precludes such use. One appellate court has so held. United States v. Vest, 813 F.2d 477 (1st Cir. 1987).

By contrast, another appellate court has held that section 2515 does not bar the government from using recordings made by an illegal gambling business (of bets placed by telephone) to prevent disagreements with bettors over the amounts of their bets. United States v. Underhill, 813 F.2d 105 (6th Cir.), cert. denied, 484 U.S. 821, 846 (1987). While the court in Vest acknowledged that no deterrent purpose would be served by suppression because the government played no role in the illegal recording, it relied on the fact that further disclosure in court of the contents would magnify the original privacy violation. The court in Underhill, on the other hand, relied on clear legislative history indicating that Congress, despite the facial breadth of section 2515, did not intend to permit lawbreakers to immunize themselves from prosecution by the very criminal purposes that made the recordings illegal.

The same disagreement among circuit courts exists regarding the admissibility of recordings made by private actors intercepting communications without the consent of any of the parties. In one case, a court barred the use before a grand jury of such illegally intercepted communications. See In re Grand Jury, 111 F.3d 1066 (3d Cir. 1997). By contrast, where a wife secretly installed a recording device to intercept her husband's conversations with other persons, the Sixth Circuit concluded that section 2515 did not bar the use of the contents of those

communications in a prosecution of the husband, given the government's lack of involvement in the original interception. See United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995).

Whether or not Vest and In re Grand Jury were correctly decided under the existing statutory provision, an exemption should be created under section 2515 for that narrow class of cases in which the government lawfully obtains illegal recordings made by private parties and seeks to use them as evidence in a criminal investigation, proceeding, hearing or trial, or before a grand jury. The truth-seeking function of a criminal proceeding is of paramount importance. In the absence of any deterrent purpose to be served by exclusion, this truth-seeking function should prevail over the concern that disclosure in the criminal proceeding would somehow exacerbate the original illegal recording.

Conversely, if evidence contained in an illegally intercepted recording tends to exculpate a defendant, that defendant should be entitled to introduce the evidence so long as he did not participate in the interception in any way. The instant amendment thus reflects the belief that a private violation of the statute should not trigger the severe result of exclusion of otherwise probative evidence in a criminal case (just as the Fourth Amendment, of course, does not apply to non-governmental searches and seizures[8]). Accordingly, this section would amend section 2515 to expressly exempt such disclosures from its purview.

In addition, the amendment would also clarify that illegal intercepts made be used for the limited purpose of prosecuting the individual who conducted the illegal interception. In one recent case, United States v. Grice, 37 F. Supp. 2d 428 (D.S.C. 1998), an employee of a county sheriff's department illegally intercepted conversations between two prisoners and their attorneys. When the United States sought to use the recording of prosecute that violation, the district court ruled the evidence inadmissible. The amendment would permit such use for the purpose of prosecuting the violator of chapter 119. Conforming amendments are also made of subsections (1) and (2) of section 2517 and subsection 2518(10)(a).

[8] The history of section 2515's original enactment makes clear that Congress intended that it embody existing Fourth Amendment standards. See S. Rep. No. 1097, 90th Cong. 2d Sess., reprinted in 1968 U.S.C.C.A.N. 2112, 2185 (no intention "of press the scope of the suppression role beyond present search and seizure law").

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

5. Emergency Pen Register/Trap and Trace authority at field level.

EXECUTIVE SUMMARY

Amendment Creating Emergency Pen Register/Trap & Trace Authority for US Attorneys and Top Law Enforcement.

Under current law, 18 U.S.C. § 3125(a), an emergency pen register or trap & trace may be authorized only by certain high level DOJ officials or "any investigative or law enforcement officer specially designated by the Attorney General" or, in cases involving the States, the equivalent of the County District Attorney. Emergency pen register or trap & trace orders are authorized under section 3125(a) only when there exists an immediate danger of death or serious bodily injury to any person, or where there are conspiratorial activities characteristic of organized crime. And this bill will add two other emergency circumstances to bring the pen register statute in relative parallel with the wiretap emergency provisions and to acknowledge that attacks on certain government or public computer infrastructure could seriously endanger the public health or safety.

Even in emergency situation, a court order ratifying the use of the pen register or trap & trace must be sought and obtained within 48 hours. Since the current statute authorizes the issuance of an emergency pen register at the State level by any County District Attorney, it has been argued that the current restrictions on emergency deployment by Federal authorities are, by comparison, incongruous, unnecessarily restrictive, cumbersome and time consuming. Based upon law enforcement's experience, the problem is especially acute in dynamic computer investigations where time is frequently of the essence. The proposed amendment would, in addition to the class of DOJ officials currently authorized to issue emergency pen registers or implement trap & trace, statutorily authorized the issuance of emergency implementation upon the request of either a "United States Attorney or the principal supervising law enforcement officer of any Federal criminal investigative agency."

Designating the United States Attorney or the principal supervising law enforcement officer with the authority to conduct a pen register or trap and trace in an emergency situation vests authority with the official who is in the best position to assess the need and propriety of use when the passing of mere minutes may mean the loss of valuable information, for example, in an ongoing computer attack. At the same time, this express designation will continue to assure the consistent administration of law enforcement policy on the use of pen registers and trap and trace devices by retaining centralized responsibility for approving emergency use in a limited number of identifiable and politically accountable officials.[9]

---

[9] S. Rep. No. 1097 90th Cong. 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185 (approval level for wiretap applications).

EXPEDITING EMERGENCY PEN REGISTER AND TRAP & TRACE IMPLEMENTATION

(Exclusive of any other Amendments)

Section 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, ~~any investigative or law enforcement officer, specially designated by~~ the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, ~~or~~ any Deputy Assistant Attorney General, any United States Attorney or the principal supervising law enforcement officer of any Federal criminal investigative agency, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

5. Title III Wiretap Exception for the Interception of Unauthorized Computer Trespassers Only upon the Written Request of the Owner/operator of the Computer System.

COMPUTER TRESPASSER INTERCEPTION EXCEPTION

(Irrespective of other Amendments)

[18 U.S.C. §2511]

(2)(a)(iii) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser, provided that-

(A) the owner or operator of the protected computer authorizes in writing the interception of the computer trespasser's communications on the protected computer;

(B) the person acting under color of law is lawfully engaged in an ongoing investigation;

(C) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the ongoing investigation; and

(D) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

[18 U.S.C. §2510]

(19) "computer trespasser" means a person who has no reasonable expectation of privacy in any communication transmitted to, through, or from a protected computer because such person is accessing the protected computer without authorization.

PROPOSED LEGISLATIVE HISTORY FOR COMPUTER TRESPASSER INTERCEPTION EXCEPTION

The amendment allows, but does not require, owners and operators of either public or private electronic or wire communication services to authorize law enforcement to intercept the communications/transmissions of a party, person or computer who the owner or operator of that service has first determined and certified is an unauthorized user on that computer system or network. The amendment is premised upon and acknowledges the legal conclusion that unauthorized users (e.g., hackers), not unlike burglars who've illegally entered a private dwelling, do not possess an expectation of privacy in their unauthorized communications which society deems reasonable or which should be protected by statute. The amendment imposes the formal requirement that the consent of the owner or operator be both prior and written so as to deter casual utilization of the exception.

(01/26/1998)

66-1
67C-1 [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 07/21/2000 **Date:** 07/17/2000

To: Director's Office **Attn:** Deputy Director's Office
Mr. Pickard
Laboratory Division Dr. Kerr
Office of General Counsel Mr. Parkinson

From: Director's Office
Office of Public and Congressional Affairs
Congressional Affairs Office
Contact: SSA [redacted] Ext. [redacted] 66-1 67C-1

Approved By: Pickard Thomas J
Kerr Donald M
Parkinson Larry R
Collingwood John E [redacted] 66-1 67C-1

Drafted By: [redacted]

Case ID #: 62C-HQ-1077728 (Pending)

Title: **ACTION MEMORANDUM:**
HOUSE JUDICIARY COMMITTEE;
CONSTITUTION SUBCOMMITTEE;
HEARING ON "FOURTH AMENDMENT ISSUES RAISED BY THE FBI'S 'CARNIVORE' PROGRAM"
07/24/2000

Synopsis: The Constitution Subcommittee of the will conduct a hearing on Monday, 07/24/2000, at 1:00 PM, in Room 2141 of the Rayburn House Office Building. The purpose of the hearing is to examine "Fourth Amendment issues raised by the FBI's 'Carnivore' program." Consequently, the Subcommittee has requested that Laboratory Division Director Dr. Donald M. Kerr and General Counsel Larry R. Parkinson appear on behalf of the FBI.

Details: The Constitution Subcommittee will conduct a hearing to examine Fourth Amendment issues raised by "Carnivore." The Subcommittee has preliminarily advised that the hearing will be composed of two panels. The first panel will have witnesses from the U.S. Department of Justice (DOJ), to include the FBI. The second panel will be composed of individuals from private industry and Internet privacy groups. It is anticipated that Deputy Assistant Attorney General Kevin DiGregory, as well as David Green from CCIPS, will represent the Department. The specific private sector witnesses have not yet been determined.

DOC #3

To: Director's Office From: Director's Office
of Public and Congressional Affairs
Re: 62C-HQ-1077728, 07/17/2000

The Subcommittee has requested that the Laboratory Division and the Office of the General Counsel provide a written statement for the official record which the witnesses may summarize for the Subcommittee. The written statement must also be provided to the Subcommittee on a computer disk or through email. These items must be provided to the Subcommittee no later than Friday, 07/21/2000. A letter of invitation from the Subcommittee has not yet been received.

LEAD(s):

Set Lead 1:

DIRECTOR'S OFFICE

AT WASHINGTON, DC

It is requested that the Deputy Director approve Dr. Kerr and Mr. Parkinson's participation as witnesses at captioned hearing.

APPROVE _____
DISAPPROVE _____
SEE ME _____

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

It is requested that the Laboratory Division prepare testimony, with assistance from the Office of General Counsel, for Dr. Kerr and provide it to SSA [redacted] Room [redacted] Extension [redacted] by COB 07/19/2000, in order that it may be transmitted to DOJ for clearance and then to the Subcommittee in a timely fashion. 6C-1 67C-1

To: Director's Office From: Director's Office
of Public and Congressional Affairs
Re: 62C-HQ-1077728, 07/17/2000

Set Lead 3:

GENERAL COUNSEL

AT WASHINGTON, DC

It is requested that the Office of General Counsel assist the Laboratory Division, as needed, in the preparation of testimony for captioned hearing.

Set Lead 4:

OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS,
CONGRESSIONAL AFFAIRS OFFICE

AT WASHINGTON, DC

The Congressional Affairs Office will coordinate the appearances of Dr. Kerr and Mr. Parkinson before the Subcommittee; the approval of the testimony from the Deputy Director's Office; and the veting of the testimony by DOJ.

b6-1
b7C-1

1 - Mr. Pickard
1 - Dr. Kerr
1 - Mr. Parkinson
1 - Mr. Allen
1 - [redacted]
JCS
(13)

1 - Mr. Bucknam
1 - [redacted]
1 - [redacted]

1 - Mr. Collingwood
1 - [redacted]
1 - CAO File Copy

♦♦

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #4 FROM THE OGC/FLU FILE (PAGES 162 + 163)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #4 (Pages 364-365)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

The New York Times

DATE: 7-18-00

PAGE: A-1

PROPOSAL OFFERS SURVEILLANCE RULES FOR THE INTERNET

INTERCEPTION OF E-MAIL

White House Tries to Balance Rights of Computer Users and Law Enforcement

By STEPHEN LABATON
with MATT RICHTEL

WASHINGTON, July 17 — The White House said today that it would propose legislation to set legal requirements for surveillance in cyberspace by law enforcement authorities similar in some ways to those for telephone wiretaps.

Privacy advocates and civil liberties groups welcomed some aspects of the proposal but said they remained alarmed about a new F.B.I. computer system that searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes.

The legislative proposal was made as the administration also announced today that it had eased export controls on encryption technology, making it significantly easier for American companies to sell software products to the European Union and eight other trading partners that can be used to keep computer data and communications secure.

Both the electronic surveillance proposal and the export control changes are part of a broader policy outlined in a speech today by John D. Podesta, the White House chief of staff. He said the policy tries to balance the privacy rights of computer users against the needs of law enforcement to be able to monitor digital communications.

Congress and federal regulators have done little work in the area, even as the world has quickly come to rely heavily on communications through cyberspace. More than 1.4 billion e-mail messages change hands every day.

The administration's legislative proposal on electronic surveillance tries to fix the inconsistent patchwork of laws that apply different standards to telephone, cable and other technologies with a single standard for those systems and the Internet. Prospects for the proposal in Congress are uncertain.

Until now, law enforcement agencies have been able to monitor electronic communication with only modest court supervision.

The proposed legislation would require that the same standards that apply to the interception of the content of telephone calls apply to the interception of e-mail messages. Specifically, it would require law enforcement agents to demonstrate that they have probable cause of a crime to obtain a court order seeking the contents of a suspect's e-mail messages.

The proposal would also give federal magistrates greater authority to review requests by law enforcement authorities for so-called pen registers — lists of the phone numbers called from a particular location and the time of the calls. The magistrates now have no authority to question the request for such lists, which are frequently used by the authorities.

In the context of the Internet, existing laws are ambiguous about what standards apply for different kinds of surveillance. Many limitations imposed on law enforcement in the context of telephone wiretaps — like the requirement that such taps be approved at the highest level of the Justice Department — do not appear to apply to e-mail surveillance.

Moreover, the Cable Act of 1984 sets a far harder burden for government agents to satisfy when trying to monitor computers using cable modems than when monitoring telephones. That has proved troublesome for law enforcement authorities as more Americans begin to use high-speed Internet service through cable networks. The Cable Act also requires that the target of the surveillance be given notice and an opportunity to challenge the request.

Concern that the proposals allow federal agents too much leeway.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Mr. Podesta said in a speech at the National Press Club. "Our proposed legislation would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls and cable services."

White House officials said today that they hoped the proposal would break a logjam in Congress where a variety of different measures have been introduced dealing with electronic surveillance. The administration's proposal adopts some elements of both Democratic and Republican bills.

But Congressional aides said there was too little time left in the legislative session and that the matter would in all likelihood remain unresolved until after the next term begins, in 2001.

Administration officials said the proposal would apply to communications that either begin or end in the United States. It would not apply to e-mail messages transmitted entirely outside the country.

Privacy and civil liberties groups criticized the administration's proposal because it would continue to permit the government to use a new surveillance system that the groups say may be used far more broadly than older technologies, enabling federal agents to monitor an unlimited amount of innocent communications, including those of people who are not targets of criminal investigations.

The system, used by the Federal Bureau of Investigation, is called Carnivore, so named, agents say, because it is able to quickly get the "meat" in huge quantities of e-mail messages, so-called instant messaging and other communications between computers.

Carnivore is housed in a small black box and consists of hardware and software that trolls for information after being connected to the network of an Internet service provider. Once installed, it has the ability to monitor all of the e-mail on a network, from the list of what mail is sent to the actual content of the communications.

CONT'd

DOC # 5

Marcus C. Thomas, section chief of the Cyber Technology Section of the F.B.I., said the technology was developed 18 months ago by F.B.I. engineers and has been used fewer than 25 times. Mr. Thomas said that Carnivore had potentially broad capabilities and that he understood the concerns of privacy groups.

"It can do a ton of things," he said. "That's why it's illegal to do so without a clear order from the court."

He said that most Internet service providers had cooperated with requests to use Carnivore.

Privacy groups and some Internet service providers have been deeply critical of the use of Carnivore because, once installed on a network, it permits the government to take whatever information it wants.

Moreover, the government has not said what it does with the extraneous material it gathers that is not relevant to the particular surveillance.

The issue does not often arise today with the monitoring of telephone conversations because when a law enforcement authority wants to see a list of telephone calls made by a suspect, the agent gets an order from a magistrate, presents the order to a telephone company, and the company then turns over the list.

In at least one instance, an Internet company did not cooperate so readily with the government. In December, federal marshals approached the company with a court order permitting them to deploy a device to register time, date and source information involving e-mail messages sent to and from a specified account.

Trying to establish a single standard for different technologies.

Concerned the device would record broader information, the company countered with a compromise: it would provide the government with the requested information about e-mail senders and recipients, according to Robert Corn-Revere, a lawyer for the company, in recent Congressional testimony. The company was later identified as EarthLink, a service provider with 3.5 million subscribers.

Mr. Corn-Revere said the government initially accepted the compromise but later became dissatisfied and wished to use its own device. EarthLink objected but was overruled by a a federal court, which ordered the device deployed.

Other Internet companies have also been critical of Carnivore.

William L. Schrader, chairman and chief executive of PSINet, a major commercial Internet service provider, said that the system gave the F.B.I. the ability to monitor e-mail messages of every person on a given network. He said he would refuse to permit the government to use the technology at PSINet unless agents could prove that it could only sift out the traffic from a given individual that is the target of a court order.

"I object to American citizens and any citizens of the world always being subject to someone monitoring their e-mail," said Mr. Schrader, whose company serves about 100,000 businesses and more than 10 million users. "I believe it's unconstitutional and I'll wait for the Supreme Court to force me to do it."

Civil liberties groups, meanwhile, said that today's policy announcement was an inadequate response to the growing controversy over the deployment of Carnivore.

"Today's speech was camouflage to cover the mess that is Carnivore," said Barry Steinhardt, an associate director of the American Civil Liberties Union. "In light of the public and Congressional criticism of Carnivore, we had hoped and expected far more from an administration that likes to tout its sensitivity to privacy rights. Rather than glossing over Carnivore, Podesta should have announced that the administration was suspending its use."

Facing growing concerns about Carnivore, Attorney General Janet Reno said on Thursday that she would review whether the system was being used in a manner consistent with privacy rights in the Constitution and in federal law. A subcommittee of the House is set to hold a hearing next week on the system.

While the civil liberties and privacy groups applauded giving judges greater discretion to review certain kinds of requests for surveillance, they were critical of other aspects of the proposal.

Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology, criticized the administration for lowering the standards for surveillance of cable modems rather than raising the standards for telephone surveillance.

"The Cable Act provides for one of the best privacy protections in the United States," Mr. Rotenberg said. "The question is whether to harmonize up or harmonize down. Our view is this harmonizes down."

But administration officials said the Cable Act never contemplated that there would be broad use of cable modems for e-mail traffic and that the standards used for obtaining warrants for telephone surveillance should also apply to digital communications through cable networks.

2

The Washington Post

DATE: 2-18-00
PAGE: E-1

U.S. Hopes to Extend Online Wiretapping

By John Schwartz
Washington Post Staff Writer

The Clinton administration yesterday called for updating wiretapping laws to extend the powers of law enforcement to the online world while providing new legal protections for electronic communication.

Administration officials also announced, as expected, a plan to loosen controls on the export of encryption software—the programs that help Internet users scramble messages and data to protect them from prying eyes.

On the wiretapping issue, White House chief of staff John D. Podesta, in a speech at the National Press Club, described the coming legislative package as seeking to eliminate confusion about the level of legal protection for various forms of communication.

Telephone conversations get fairly strong protection from federal wiretaps under the 1968 Crime Patrol and Safe Streets Act, which required a court order and high-level Justice Department approval. Wiretape rules for e-mail sent by dial-up modem are covered by the Electronic Communications Privacy Act of 1986. That law might not cover e-mail sent by high-speed cable modem, and cable companies have argued that their online services should be given extremely high protection from government surveillance under the Cable Act.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Podesta said.

Lawmakers said they welcome the opportunity to work with the administration on these issues. Sen. Orrin G. Hatch (R-Utah), who has introduced an Internet privacy bill, said: "It is imperative that we balance the interests of law enforcement with the privacy rights of the American people. We must ensure that appropriate checks are in place where the government accesses private communications of Americans."

Podesta said the bills making up the package would be unveiled within 10 days, and that he hopes the legislation can be passed by the end of the year.

Podesta also spoke about the new surveillance technology known as Carnivore, which gives law enforcement authorities the ability to selectively monitor the Internet traffic of individuals, similar to the devices that can record the telephone numbers of calls made and received by a suspect. Unlike full-fledged wiretaps, the judicial oversight of such surveillance is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for greater judicial oversight.

The Podesta speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to expand wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech "deeply disappointing. . . . While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. The Carnivore system, Steinhardt said, "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic."

Podesta also discussed the new encryption policy, which the administration can implement immediately. Under the plan, U.S. companies will be able to export sophisticated cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate the statutory 30-day waiting period before such exports can take place but will keep in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy, but few technologies present such daunting issues for law enforcement officials like FBI Director Louis J. Freeh, who often warns that criminals and terrorists can use "crypto" to cloak their plans and activities. High-tech companies successfully argued that U.S. restrictions harmed only American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports.

"The reducing of these regulations will certainly allow U.S. software makers to compete in the global marketplace," said Robert Holleyman, the chief executive of the Business Software Alliance.

3

Doc. #6

Los Angeles Times

DATE: 7-18-00
PAGE: A-8

Clinton Administration Seeks Updated Wiretapping Laws

From Associated Press

WASHINGTON—The White House proposed legislation Monday to update wiretapping rules so that legal protections currently applied to telephone calls are extended to electronic communication, such as e-mail.

The plan would require law enforcement officials to obtain high-level approval before applying for a court order to intercept the content of e-mail—in line with current rules that govern listening to phone calls.

"Basically, the same communication, if sent different ways—through a phone call or a dial-up modem—is subject to different and inconsistent privacy standards," said White House Chief of Staff John Podesta, in announcing the proposals. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations."

The wiretap proposal also addresses so-called "trap and trace" orders, which allow law enforcement officials to identify the source of a phone call or an e-mail, but not its content. Under the proposal, law enforcement officials would only need one order—even to trace an e-mail or a phone call that may travel through multiple phone carriers or Internet providers.

Officials also could trace such communications without prior approval in an emergency situation, such as when a computer is under attack.

But for the first time, the administration is proposing that a federal or state judge independently determine whether the facts support such a trace order.

Officials were asked how those changes would impact the new "Carnivore" system, which the FBI is using to obtain e-mails of investigative subjects with a search warrant. When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

If the Carnivore system is being used to intercept the content of electronic communications, then law enforcement officials would need high-level Justice Department approval before obtaining a court order and stricter standards limiting its use would apply, Podesta said.

The FBI says the tool already is subject to intense oversight from its own internal controls, the Justice Department and the courts—with signification penalties for misuse of the system.

The proposed measures also would address inconsistencies in how current law applies to different networks carrying Internet traffic. For example, now that cable systems are being upgraded to offer two-way services, laws that apply to dial-up modems over phone lines should be extended to cable connections, Podesta said.

4

DOC # 7

THE WALL STREET JOURNAL

DATE: 7-18-00

PAGE: A3

Updating of Wiretap Law for E-Mail Age Is Urged by the Clinton Administration

By Ted Bridis
Staff Reporter of The Wall Street Journal

WASHINGTON—The White House is urging changes in U.S. law to make it easier for authorities to eavesdrop on Internet communications such as electronic mail, updating what the government described as wiretap laws written for an earlier era.

The administration said that the changes would enhance legal privacy protections because they would require, for example, approval by senior Justice Department officials before the Federal Bureau of Investigation could use software surveillance, such as its "Carnivore" system. That approval already is required in cases where law enforcement wants to monitor telephone conversations.

The changes require U.S. judges to suppress electronic evidence obtained by illegal wiretap; current law mandates suppression in such circumstances of only oral or written communications, not e-mail. The proposals were all made by the Justice Department in a March study that identified what the government said were deficiencies in enforcing laws against crimes on the Internet.

The American Civil Liberties Union said the White House announcement was "deeply disappointing," because it did not include any promise to suspend use of Carnivore, which the group charged gives the government "unsupervised access to a nearly unlimited amount of communications traffic."

The Internet Alliance, a Washington trade group for Internet providers, said the White House proposals "make sense," but also warned that its member companies "should not be deputized," a spokesman said.

The proposals were announced at the same time that the administration relaxed restrictions on the export of powerful encryption technology to the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. White House Chief of Staff John Podesta said the change, which will benefit some U.S. hardware and software firms, was not offered in exchange for the high-technology industry's support of the White House wiretap proposals. "We've never tried to link those two," he said.

The White House also sought to give authorities undisputed access to the Internet traffic of roughly 2.2 million consumers using cable modems. And it proposed making it easier for police to obtain court orders to trace the transmission and receipt of Internet data nationwide without asking permission from a judge in every jurisdiction the data passes through. Another change would give judges greater latitude in denying those requests. But in extraordinary cases, such as a hacker attack, the FBI could perform tracing, then obtain court approval as much as 48 hours later.

A legal dispute continues between Internet providers and law enforcement. The nation's cable Internet providers have argued that they are not required under the

Please Turn to Page A6, Column 3

U.S. Cable Act to turn over subscriber information without giving customers the opportunity to fight the disclosure in court. However, the Justice Department argues it is entitled to cable Internet data under the Electronic Communications Privacy Act without warning the customer in advance about its proposed surveillance.

U.S. District Judge J. Young of Boston called the dispute "a thorny and important issue" in a case last year, in which he ordered an unidentified cable Internet provider to turn over the customer's records. Judge Young acknowledged that his decision should not be read too broadly, saying that it was "not the day to resolve such ephemeral puzzles."

Tapping Into Privacy

Some key changes the White House is seeking on Internet privacy:

- **Requiring higher level approval** by senior Justice officials to perform Internet wiretaps to read e-mail.
- **Requiring judges to discard** electronic evidence obtained in an illegal wiretap.
- **Mandating that Internet wiretaps** to read e-mail be used only when investigating the most serious crimes.
- **Requiring cable-Internet companies** to turn over customer information when presented with a judge's order.
- **Allowing authorities** to seek a single judge's order to trace Internet communications nationwide across different jurisdictions.

5

Doc. #8

Los Angeles Times

DATE: 7-18-00
PAGE: A-1

Restrictions Eased on Encryption Software Exports

By ASHLEY DUNN
and CHARLES PILLER
TIMES STAFF WRITERS

The Clinton administration on Monday further eased the remaining restrictions on selling high-powered encryption products overseas, clearing the way for American firms to export to the European Union and several other key trading partners.

The new policy drops a requirement that U.S. companies get a special license to sell encryption products—a process that previously involved a technical review or a 30-day delay.

In addition, the rules allow companies to sell their products to not only businesses and consumers, but also government agencies, which used to require a special license.

The rules apply to encryption exports to the 15 nations of the European Union, as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland.

The new rules follow the administration's major turnaround in January, when it finally opened the way for companies to export the hardest-to-crack scrambling technology.

American technology companies and privacy advocates had fought for years for permission to export its encryption technology abroad.

The industry argued that the spread of strong encryption would fuel electronic commerce and reassure consumers that their credit card numbers and other private communications would not be compromised.

White House Chief of Staff John Podesta, speaking at the National Press Club, described the changes announced on Monday as part of an ongoing effort to update U.S. policy.

"The Internet, like Morse's telegraph, brings with it new possibilities," he said. "It also brings new challenges to our most fundamental values and the need for new laws and new protections to maintain them."

Industry and security experts welcomed the latest announcement as another sign of the federal government's new-found support of liberalizing encryption exports.

"It's obviously very important if U.S. software companies are going to compete in the global market," said Amit Yoran a former Department of Defense security official and president of RipTech, a security company in Alexandria, Va.

According to Scott Schnell, senior vice president of RSA Data Security, a top encryption software producer, the new rules are important because they remove restrictions to selling to national governments.

Governments are often the biggest buyers of security software, particularly in the recently democratized nations of Eastern Europe.

"Both the relaxation and normalization around government use of the technology is a realization of the core importance of the security over the Internet," Schnell said. "This is a tremendous boost for the U.S. software industry."

But others said that until the regulations can be thoroughly reviewed by legal experts, their impact would be uncertain.

"The devil in this case is in the details," said Jeff Schiller, a leading security expert and network manager for Massachusetts Institute of Technology. Law enforcement and safety concerns remain, he said. "How are those addressed? I'd be very surprised if they were just lifting the controls."

He said that he suspects hidden restrictions could still bar the export of such products to the wrong countries.

"Let's say someone in one of the forbidden countries gets an account on America Online," Schiller said. "When they use their Web browser to get on the Net, it's going to say Virginia [where many AOL server computers that route Internet traffic are located]. I don't know they are from Libya. Under those circumstances who is responsible? Am I responsible? Is AOL responsible?"

But Schiller said that any relaxation of export controls is an acknowledgment of reality.

"You cannot turn the tide of technology back," he said. "The bad guys are going to do what they will do," while legitimate users of encryption products are harmed by export controls.

6

Doc #9

USA TODAY

DATE: 7-18-00
PAGE: 4-A

Rules on encryption exports are relaxed

The United States has eased its rules on exporting encryption products to the European Union and other key trading partners in an effort to improve security in cyberspace and promote electronic commerce, the White House said Monday.

By Dennis Cook, AP

Podesta: Change should not threaten U.S. security.

U.S. companies no longer need an export license to sell encryption products to users in the key trading countries, the White House said.

The policy allows U.S. exporters to ship their products without waiting for a technical review or a 30-day delay as they have in the past. Businesses and privacy advocates had said that U.S. export rules were too restrictive, but law enforcement officials said sophisticated encryption aids international criminal enterprises and terrorists. White House Chief of Staff John Podesta said the changes should provide adequate security.

The White House also proposed legislation to update wiretapping rules so that protections currently applied to telephone calls are extended to electronic communications such as e-mail. The changes could affect the system the FBI uses to access the e-mails of criminal suspects. Investigators would have to obtain high-level approval before seeking a court order.

7

Doc. # 10

The Washington Post

DATE: 7-16-02
PAGE: A-1

House Rejects Bill Limiting Web Gambling

Parties Sharply Divided; White House Opposed

By Dan Morgan
and John Schwartz
Washington Post Staff Writers

The House last night defeated a bill that would have banned most forms of online gambling, legislation intended to curb the explosive growth of casino-style wagering on the World Wide Web.

In a vote that reflected sharp divisions within both major parties over the issue, 44 Republicans joined 114 Democrats and one independent to defeat the measure. Under a procedure to bring the bill to the floor without amendments, a two-thirds vote of those present was required to pass the legislation. The final tally of 245 to 159 fell 25 votes short of the 270 needed.

The bill drew opposition from lawmakers and advocates concerned about federal regulation of Internet content, as well as the potential for invasion of privacy. Critics also raised concerns that to make the legislation palatable to the politically influential parimutuel horse racing and dog racing industries, GOP leaders had agreed to exemptions that would actually legalize an expansion of opportunities for online gambling.

The bill was intended to address growing fears among lawmakers about the explosive growth of unregulated online sites where individuals can engage in card games and other casino-style gambling on their computers. More than 700 such sites, many of them run out of foreign countries or offshore havens, are now operating without regulation, with roughly $1.2 billion wagered annually.

Under the bill defeated yesterday, state law enforcement agencies would have been able to go to court to obtain orders requiring Internet service providers to block access to Web sites that engaged in illegal gambling.

Before last night's vote, Rep. Robert W. Goodlatte (R-Va.), chief sponsor of the bill, cited a litany of social ills linked to gambling—crime, bankruptcy, addiction and more—and said that Internet gambling will bring citizens the same problems "as you would have if you had a casino in your home town."

But the White House said it "strongly" opposed the bill and stressed in particular its objections to the exemptions that would allow the parimutuel industry to conduct online betting under controlled conditions.

Although the Senate has passed a similar bill, it appeared unlikely last night that the GOP leadership in the House will attempt to bring the measure back to the House again this year given the limited time and the difficulty of crafting a compromise on such a complex issue.

Yesterday's vote was the culmination of one of the year's most hotly contested lobbying battles on Capitol Hill, generating a variety of strange alliances on both sides. Allied with the Las Vegas casino industry in support of the bill have been religious groups that are among the GOP's core group of supporters, including the Christian Coalition, the Southern Baptist Convention, the Family Research Council, and Focus on the Family.

But the booming high-tech industry, which the GOP is also courting, had serious concerns, and a number of governors objected that the legislation would not provide an exemption for state lotteries to sell tickets online within their own states.

Meanwhile, horse and dog racing venues have been fighting declining attendance, and stiffer competition from other forms of betting. They saw the bill as a way to ensure their long-term survival by allowing them to market their events over the Internet.

Goodlatte assured House members yesterday that the parimutuel provisions only authorized what is already legal under federal gambling law, and did not constitute an expansion. Action, he said, was essential on the larger issue of casino-type gambling.

But the White House charged that bill would have heightened the likelihood that children and other vulnerable groups would be able to get unsupervised, unlimited access to gambling activities on home computers.

"This bill appears to be designed to protect certain forms of Internet gambling that currently are illegal, while potentially opening the floodgates for other forms of illegal gambling," the White House said in a statement.

Along with concerns about the parimutuel betting provisions, some lawmakers in both parties expressed reservations about the extent of federal incursion into the prerogatives of the states.

"You would have the federal government dictate to Internet service providers what services they can offer," said Rep. Christopher Cox (R-Calif.) in opposing the legislation. He said it was "well-intentioned," but would "create enormous regulatory problems."

Goodlatte and the House GOP leadership sought to win more support for the bill with last-minute changes aimed at relieving some of the concerns of civil liberties groups. Rep. Jerrold Nadler (D-N.Y.) agreed to support the legislation only after language was added giving the operators of Web sites that have been shut down by court order up to 60 days to appeal.

Yesterday's outcome represented another in a series of sometimes awkward attempts by Congress to address the controversial issue of regulating Internet content. The Supreme Court struck down as unconstitutionally broad the 1996 Communications Decency Act, which made it a federal crime to make adult materials available to minors via computer.

Congress came back with the Child Online Protection Act, a narrower attempt to regulate commercial sites showing pornography on the World Wide Web. That law has been challenged by civil liberties groups and publishers, and is currently before federal appellate courts.

8

Doc. #11

THE WALL STREET JOURNAL

DATE: 7-19-00

PAGE: A-22

'Carnivore' Won't Devour Cyber-Privacy

By Bruce Berkowitz

On Monday the White House proposed new legislation regulating surveillance by law enforcement agencies on the Internet. But civil libertarians are already complaining that this plan does little to address the problems ostensibly raised by Carnivore, the FBI's new software system for performing court-ordered wiretaps at Internet service providers (ISPs).

Using a laptop computer, law enforcement officials can hook Carnivore into an ISP's network. Once installed, it reads the headers of each e-mail message—listing the sender, recipient and subject of the message—as it passes through. If the sender or recipient is the target of a tap, Carnivore records the message.

Rights at Risk?

Here's the rub: Before Carnivore can know whether a message belongs to a targeted party, it must browse the headers of all the messages passing through the ISP. With a traditional phone tap, law enforcement officers only listened to the telephone line that the subject of the tap was using. The ACLU and other critics complain that when Carnivore reads the headers of anyone who is not a target it violates their rights.

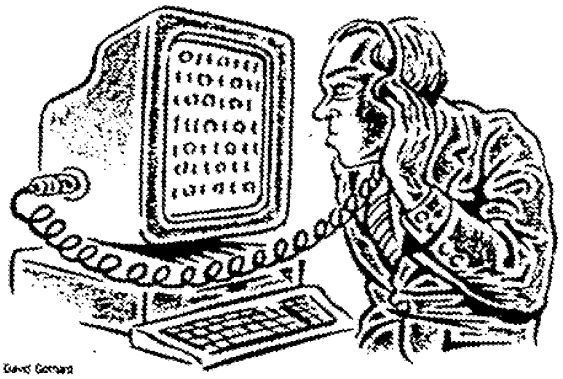
The ACLU and other Carnivore critics need to get a grip—and a better understanding of the new technology.

Unlike old-fashioned analog telephone calls, e-mail messages are transmitted digitally. A computer slices and dices the message into packets, each with an identifying tag. The packets then spread out throughout the Internet, finding the most efficient path to the destination. When they arrive, they are reassembled, and the recipient gets the message. As a result, with e-mail, you cannot "tap a line" because often there is, literally, no particular line to tap. All you can do is scan the messages that pass through a link a suspect is known to use—like his ISP—and pick out the ones that belong to him. That's what Carnivore does.

The ACLU complains that using a computer to monitor an ISP system would collect vast amounts of innocent data. But what do they expect the feds to use—a typewriter and an abacus? Note to FBI: Hire a better public relations firm, and name your next project "Vegetarian."

These kinds of flaps are happening more and more often. Last April some privacy advocates complained when the FBI requested $15 million for "Digital Storm," a program for monitoring telephone calls and analyzing recordings. In September, a programmer in North Carolina found the notation "NSA Key" in a Microsoft software patch. Soon rumors bounced through the Internet claiming Windows had a back door that allows the National Security Agency to monitor your computer. (Microsoft explained that the tag merely signified that the software complied with the agency's security standards.)

There's a lot of concern about the ability of governments to monitor communications in the digital age. In fact, it's getting harder, not easier, for them to listen in.



David Gothard

The granddaddy of all bogus fears, though, is Echelon. If you believe some European Union parliamentarians, the United States and Britain operate an international network that monitors virtually all communications, and extracts choice nuggets with powerful computers that recognize key phrases in messages like "assassination," "terrorist attack" or "industrial secret."

In reality, it's not easy to find a specific message in a flood of free-flowing digital data. That's the whole reason for getting a court order for a wire tap. If you cannot hook into an ISP, you have to do a lot of searching to find the message you want to intercept.

That is also why the European campaign against Echelon is so quixotic. True, the folks at NSA intercept communications and they have powerful computers and ingenious software that helps with the processing. But it is impossible for even the best computer system to routinely sort through all of the world's telecommunications and pull out telltale messages, as the Echelon paranoids would have you believe.

Usually you need to know what you are looking for and where the message might appear before you have much of a chance of finding it. Also, the cases in which one message tells a whole story are rare. Good law enforcement and intelligence usually requires multiple sources and collateral information to make sense of an intercept.

The privacy advocates have the story reversed. It's getting harder, not easier, for our law enforcement and intelligence organizations to listen in on communications. In the old days you could tap a line or intercept a microwave link. It's much more difficult to capture digital messages that pass over fiber optics or bounce through cellular networks. And, with strong encryption software freely available world-wide, anyone really determined to keep a message secret can usually do so.

If you have any doubts, just recall how many intelligence surprises we have had lately—the Indian nuclear test, the North Korean missile test, the terrorist bombings of American targets in the Mideast and Africa. Part of the problem is that we cannot get to many of the sources that we used to, and everyone is getting better at concealing their communications.

57

cont-d

So why is it so easy to stir up these controversies about privacy? The simple fact is that relations between the government and the new information industries are lousy. There is too much suspicion and too little communication.

The administration gets part of the blame for its ham-handed policies. Carnivore is a good example. A lot of controversy could have been defused if the FBI had offered more insight into how the system worked and how the rights of non-suspects would be protected.

But the record of the technogeeks has not been much better. They often act as though law enforcement officials have no business poking into their activities at all—as though one could stop international computer criminals with a good neighborhood watch program.

It's all too easy to lose sight of the fact that Carnivore's main targets are cybercriminals—in other words, the kinds of crooks who are a plague on the Internet and target dot-com companies. Growth rates for Internet shopping have been slipping lately. According to some experts, people worry about whether their credit card numbers and health records are safe. You would think that e-business would be the first to support better law enforcement on the net.

Common Goals

All the good guys in this dispute have common goals. Defense and intelligence officials want to protect the nation's communications infrastructure. Law enforcement officials want to chase crooks, and companies want the cops to catch them. Consumers want privacy. The path to all is the same: secure information systems, reasonable cooperation from the private sector, and aggressive law enforcement and effective intelligence closely monitored by responsible public officials.

Fixing the relationship between Washington and Silicon Valley needs to be a top priority for the next administration. The only people benefitting from controversies like the one over Carnivore are terrorists, criminals and rogue states.

Mr. Berkowitz is a research fellow at the Hoover Institution and coauthor of "Best Truth: Intelligence in the Information Age" (Yale University Press, 2000).

58

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #8, OGC FRONT OFFICE FILE (pgs 849

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #13 (pages 376-377)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Questions for the Record
June 20, 2000

Senator Kyl:

Q: Is the NIPC able to provide indications and warnings of an attack? For example, does the Center have the ability to detect anomalous activity or patterns in key communications nodes that might indicate something is about to happen?

The NIPC's ability to perform "indications and warning" is dependent first and foremost on its ability to quickly gather information from multiple sources about an ongoing or imminent attack (whether an intrusion, a virus, a denial of service, or other form of attack). The NIPC does not operate any detection mechanisms on any government or civilian systems. Thus, we do not get "indications" in an automated sense from any detection devices. In this sense, I&W in the cyber world is very different from I&W in the nuclear missile or conventional weapons world, where radars and other devices can provide advanced warning of an attack. Rather, we get relevant information from intelligence sources, criminal investigations, "open sources" (such as media and the Internet), and from industry and government contacts. We "detect" anomalous activity in key communications nodes only if the owner/operator of that node detects it and informs the NIPC, an FBI Field Office, or another agency, or if we learn through criminal investigation or intelligence sources that the node is being attacked. The key to the NIPC's ability to do this is the development of connectivity and close interaction with numerous Defense and Intelligence Watch centers, FBI Field Offices, other Law Enforcement organizations, computer anti-virus association groups, private and public Computer Incident Response Teams (CIRTs) and Computer Emergency Response Teams (CERTs), foreign law enforcement agencies, and private industry (both individual companies and information sharing organizations). Over the past two years, the NIPC has made substantial progress in developing these relationships, but this is a continuing task and more work remains to be done. One of the main reasons for our extensive outreach programs is to build trust and willingness on the part of private companies to report cyber incidents to us, and these efforts are bearing fruit. In addition, PDD-63 directs other federal agencies to report incidents to the NIPC directly. Many agencies are doing this, but there is room for improvement with others. In addition to reports from companies and agencies, the NIPC Watch actively scans all available governmental and private sector sources for reports or information regarding cyber activity, and interacts throughout each day with other watch centers to share information.

Once information (or "indications") of an attack is received and analyzed, the NIPC can issue a warning, alert, or advisory through numerous means, depending on the appropriate audience. Warnings can be issued to specific targeted companies through FBI Field Offices or by the watch directly; other federal agencies can be notified by e-mail, secure facsimile, and telex; state and local law enforcement can be warned by NLETS; industry can be warned through InfraGard secure email and website and through ANSIR (an e-mail system that reaches tens of thousands of companies); and the general pubic can be warned via the NIPC webpage and the

Doc. #14

news media. All of these mechanisms have been used numerous times (as discussed in the answer to the next question).

Senator Kyl's question goes to the heart of I&W in the cyber world: should the Nation have the capability to detect intrusions into government or private sector systems in an automated fashion, without having to rely on human detection and reporting? The controversy attending the Administration's recent "FIDNET" initiative, which is a limited proposal to place automated intrusion detection devices on federal agency networks, identified many of the privacy and other issues such a system would raise, particularly if it were extended to privately owned networks. The government's approach at the present time is to encourage industry to protect and monitor its own systems, and to report anomalous activity voluntarily. The NIPC works within that overall policy to encourage private sector reporting as a critical part of its I&W. Examples of this include InfraGard and the incident reporting pilot program we have developed with the energy sector through the North American Electrical Reliability Council (NERC).

Q: How many warnings has the NIPC issued which were developed through the Centers's own analysis of activity?

Of the 54 tactical warning products disseminated since the NIPC was established in February 1998, all were developed in whole or in part through the Center's organic analytical capability and analysis of activity. Some of these products were initiated by the NIPC (e.g., the BAT/Firkin Worm, also known as the "911" Worm), while others built upon basic analysis initiated elsewhere (e.g., the NIPC assessments of Distributed Denial of Service tools). We cannot put a precise figure on the relative contributions, since these are all community-collaborative products. In performing analyses and issuing warnings, the NIPC works closely with other government agencies, private sector organizations such as CERT (which is an FBI contractor), and the SANS institute, and academic institutions.

In addition to warning products, the Center has produced hundreds of non-warning informational products. Since 1998 the NIPC has produced 301 daily reports, 30 CyberNotes (a summary and analysis of technical exploits and vulnerabilities), 51 Critical Infrastructure Developments reports (a report on recent cyber-related issues and incidents), and five IP Digests (a periodic, in-depth analysis of cyber threats and vulnerabilities). Versions of these analytical products go to private industry, to the Intelligence Community, other federal agencies (including law enforcement), and to criminal investigators.

Q: What other agencies do you see playing a significant role in the area of computer crime investigations?

Cyber crime is an issue that concerns not just the FBI, and not just law enforcement generally. Indeed, "cyber crime" in itself should be seen as part of a broader array of cyber threats, including cyber terrorism, cyber espionage, and information warfare, since all are closely related and often difficult to distinguish at the outset of an incident. As a result, cyber threats are

of great concern to numerous federal agencies, including the Defense, Intelligence, and Law Enforcement Communities and to civilian "Lead Agencies" under PDD-63; to state and local governments, including law enforcement; and, of course, to the private sector. It is because of this wide-ranging interest that the NIPC was established as an interagency center. The NIPC provides a locus and mechanism for coordinating the expertise and roles of many agencies, and facilitates information sharing and operational coordination. The NIPC works closely on investigative matters with many law enforcement agencies, including: the Secret Service, Internal Revenue Service (IRS), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), United States Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), National Aeronautics and Space Administration Office of Inspector General (NASA OIG), Department of Energy (DOE), state and local law enforcement, the Intelligence Community, as well as foreign law enforcement agencies through FBI Legal Attaches (LEGATS).

Q: Are there reasons, other than funding, which have caused other agencies to pull their personnel out of the NIPC? For example does FBI management at the Center recognize the expertise of the other agencies and allow them to fully participate?

One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal Investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representative from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DOE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has

not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer" cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

Q: How many criminal investigations have been referred from the NIPC to these other agencies? Does the Center have operating procedures to refer a case to another agency?

As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the "program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC). Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations

under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBI's Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complainant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

Q: In previous testimony before this subcommittee Mr. Vatis has stated that the NIPC has referred approximately 800 cases for criminal investigation. How many of these 800 cases actually involved a real threat to our nation's critical infrastructure? Would you catagorize the recent Denial of Service attacks launched last month as an attack on our nation's critical infrastructure?

In previous testimony before the subcommittee, the approximate 800 number of cases that Mr. Vatis referenced were not cases the NIPC "referred," but was the number of computer intrusion, denial of service, or virus cases pending in FBI field offices at the time of testimony. As of May 1, 2000 there were 1,072 pending investigative cases.

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus of these 1,072 cases, there is no methodology to determine which ultimately constitute a threat to our nation's critical infrastructure. However, we can cite several examples.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

Q: Besides Solar Sunrise and Moonlight Maze, what other joint investigations can you point to that demonstrate successful interagency cooperation?

Since the founding of the NIPC in February 1998, there are numerous cases which have demonstrated successful interagency cooperation other than the significant Solar Sunrise and Moonlight Maze cases. The importance of these two cases should not be overlooked, however. Both represent significant milestones in building awareness of the cyber threat among federal agencies and policymakers, demonstrated significant vulnerabilities in DoD and other government systems, and provided opportunities to test and improve the NIPC's processes for interagency coordination.

The following cases represent a small sample of these cases which have been successfully worked with other agencies:

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring a the National Aeronautics and Space Administration (NASA). These computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into the intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion attempt. Because of the credit card aspect, the FBI called the USSS to ask if USSS wanted to investigate jointly. The USSS declined. In January

2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

Other

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

Senator Feinstein:

1. Under Presidential Decision Directive 63 (PDD 63), the ..[sic... NIPC]... is supposed to take the lead in warning of, investigating, and responding to threats to or attacks on this country's critical infrastructures. NIPC includes representatives from the FBI and other law enforcement agencies. You testified that the NIPC has improved the FBI's ability to fight cybercrime and that the FBI closed 912 cybercrime cases in the Fiscal Year 1999 and had 834 pending cybercrime cases that year.

How many of the 912 closed cases involved threats to or attacks on our nations's critical infrastructures? Were these cases really a threat to our national security? What about the pending cases? How many involved threats to or attacks on our nation's critical infrastructures?

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately constitute a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on